# Отчет по безопасности сети 192.168.233.0/24

## Служебная информация:

Дата сканирования: 2024-03-25 12:01:32

Версия сканера: 1.0

Режим сканирования: TCP

Режим CVE: True

Режим сканирования всех портов: False

## Общая информация о сетевых узлах:

|  |  |  |  |
| --- | --- | --- | --- |
| Ip Адрес узла | Состояние хоста | Количество открытых портов | Общее количество CVE |
| 192.168.233.1 | up | 1 | 16245 |
| 192.168.233.1 | up | 1 | 3368 |
| 192.168.233.131 | up | 2 | 12 |
| 192.168.233.254 | up | 0 | 0 |

## Подробная информация о сетевых узлах:

### Узел 192.168.233.1/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 16245

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 135 | open | syn-ack | msrpc | [CVE-2000-0771] - Информация неизвестна [CVE-2001-0509] - Информация неизвестна [CVE-2002-1140] - Средняя [CVE-2002-1141] - Средняя [CVE-2003-0003] - Высокая [CVE-2003-0352] - Высокая [CVE-2003-0807] - Средняя [CVE-2004-0116] - Средняя [CVE-2004-0124] - Низкая [CVE-2004-0569] - Высокая [CVE-2005-3644] - Высокая [CVE-2006-0013] - Средняя [CVE-2006-0034] - Высокая [CVE-2006-2370] - Высокая [CVE-2006-2371] - Высокая [CVE-2006-2380] - Средняя [CVE-2006-3439] - Критичная [CVE-2006-4691] - Критичная [CVE-2006-6296] - Средняя [CVE-2006-6723] - Высокая [CVE-2007-1748] - Критичная [CVE-2007-2228] - Высокая [CVE-2007-3039] - Критичная [CVE-2008-3479] - Критичная [CVE-2008-4114] - Высокая [CVE-2008-4250] - Критичная [CVE-2009-0079] - Средняя [CVE-2009-0228] - Критичная [CVE-2009-0230] - Критичная [CVE-2009-0568] - Критичная [CVE-2009-1544] - Критичная [CVE-2009-2523] - Критичная [CVE-2010-2567] - Критичная [CVE-2010-2729] - Критичная [CVE-2010-2742] - Средняя [CVE-2010-3139] - Критичная [CVE-2010-3222] - Высокая [CVE-2013-3175] - Критичная [CVE-2013-3878] - Средняя [CVE-2014-0316] - Высокая [CVE-2015-2370] - Высокая [CVE-2016-0128] - Средняя [CVE-2016-0178] - Высокая [CVE-2020-1113] - Высокая [CVE-1999-0012] - Информация неизвестна [CVE-1999-0227] - Информация неизвестна [CVE-1999-0228] - Информация неизвестна [CVE-1999-0288] - Информация неизвестна [CVE-1999-0386] - Информация неизвестна [CVE-1999-0681] - Информация неизвестна [CVE-1999-0749] - Информация неизвестна [CVE-1999-0969] - Информация неизвестна [CVE-1999-1127] - Информация неизвестна [CVE-1999-1291] - Информация неизвестна [CVE-2000-0089] - Информация неизвестна [CVE-2000-0168] - Информация неизвестна [CVE-2000-0216] - Информация неизвестна [CVE-2000-0228] - Информация неизвестна [CVE-2000-0331] - Информация неизвестна [CVE-2000-0495] - Информация неизвестна [CVE-2000-0544] - Информация неизвестна [CVE-2000-0653] - Информация неизвестна [CVE-2000-0742] - Информация неизвестна [CVE-2000-0790] - Информация неизвестна [CVE-2000-0849] - Информация неизвестна [CVE-2000-0858] - Информация неизвестна [CVE-2000-0929] - Информация неизвестна [CVE-2000-0942] - Информация неизвестна [CVE-2000-1079] - Информация неизвестна [CVE-2000-1112] - Информация неизвестна [CVE-2000-1113] - Информация неизвестна [CVE-2000-1217] - Информация неизвестна [CVE-2000-1218] - Информация неизвестна [CVE-2001-0003] - Информация неизвестна [CVE-2001-0047] - Информация неизвестна [CVE-2001-0242] - Информация неизвестна [CVE-2001-0245] - Информация неизвестна [CVE-2001-0261] - Информация неизвестна [CVE-2001-0345] - Информация неизвестна [CVE-2001-0346] - Информация неизвестна [CVE-2001-0347] - Информация неизвестна [CVE-2001-0348] - Информация неизвестна [CVE-2001-0349] - Информация неизвестна [CVE-2001-0350] - Информация неизвестна [CVE-2001-0351] - Информация неизвестна [CVE-2001-0504] - Информация неизвестна [CVE-2001-0541] - Информация неизвестна [CVE-2001-0662] - Информация неизвестна [CVE-2001-0719] - Информация неизвестна [CVE-2001-0909] - Информация неизвестна [CVE-2001-1055] - Информация неизвестна [CVE-2001-1200] - Информация неизвестна [CVE-2001-1451] - Информация неизвестна [CVE-2002-0018] - Критичная [CVE-2002-0034] - Средняя [CVE-2002-0054] - Высокая [CVE-2002-0055] - Средняя [CVE-2002-0136] - Средняя [CVE-2002-0151] - Высокая [CVE-2002-0224] - Средняя [CVE-2002-0370] - Высокая [CVE-2002-0372] - Высокая [CVE-2002-0373] - Высокая [CVE-2002-0443] - Средняя [CVE-2002-0444] - Высокая [CVE-2002-0597] - Средняя [CVE-2002-0615] - Высокая [CVE-2002-0616] - Средняя [CVE-2002-0617] - Средняя [CVE-2002-0618] - Высокая [CVE-2002-0619] - Высокая [CVE-2002-0693] - Высокая [CVE-2002-0694] - Высокая [CVE-2002-0699] - Средняя [CVE-2002-0724] - Высокая [CVE-2002-0862] - Высокая [CVE-2002-0863] - Средняя [CVE-2002-0864] - Средняя [CVE-2002-1139] - Средняя [CVE-2002-1183] - Высокая [CVE-2002-1184] - Средняя [CVE-2002-1214] - Высокая [CVE-2002-1256] - Средняя [CVE-2002-1327] - Высокая [CVE-2002-1561] - Средняя [CVE-2002-1670] - Средняя [CVE-2002-1692] - Низкая [CVE-2002-1712] - Средняя [CVE-2002-1844] - Высокая [CVE-2002-1847] - Высокая [CVE-2002-1873] - Средняя [CVE-2002-1932] - Высокая [CVE-2002-1933] - Высокая [CVE-2002-1984] - Средняя [CVE-2002-2073] - Средняя [CVE-2002-2105] - Низкая [CVE-2002-2117] - Средняя [CVE-2002-2283] - Низкая [CVE-2003-0004] - Высокая [CVE-2003-0009] - Средняя [CVE-2003-0109] - Высокая [CVE-2003-0111] - Высокая [CVE-2003-0227] - Средняя [CVE-2003-0228] - Высокая [CVE-2003-0345] - Высокая [CVE-2003-0346] - Высокая [CVE-2003-0348] - Средняя [CVE-2003-0349] - Высокая [CVE-2003-0496] - Высокая [CVE-2003-0533] - Высокая [CVE-2003-0604] - Высокая [CVE-2003-0605] - Высокая [CVE-2003-0660] - Высокая [CVE-2003-0662] - Критичная [CVE-2003-0719] - Высокая [CVE-2003-0806] - Высокая [CVE-2003-0812] - Высокая [CVE-2003-0813] - Средняя [CVE-2003-0818] - Высокая [CVE-2003-0825] - Критичная [CVE-2003-0839] - Средняя [CVE-2003-0906] - Высокая [CVE-2003-0907] - Средняя [CVE-2003-0908] - Высокая [CVE-2003-0995] - Высокая [CVE-2003-1106] - Средняя [CVE-2003-1107] - Средняя [CVE-2004-0120] - Средняя [CVE-2004-0199] - Средняя [CVE-2004-0201] - Критичная [CVE-2004-0202] - Средняя [CVE-2004-0206] - Высокая [CVE-2004-0207] - Низкая [CVE-2004-0208] - Высокая [CVE-2004-0209] - Критичная [CVE-2004-0210] - Высокая [CVE-2004-0211] - Низкая [CVE-2004-0214] - Критичная [CVE-2004-0503] - Средняя [CVE-2004-0540] - Критичная [CVE-2004-0571] - Критичная [CVE-2004-0572] - Критичная [CVE-2004-0574] - Критичная [CVE-2004-0575] - Критичная [CVE-2004-0726] - Высокая [CVE-2004-0727] - Высокая [CVE-2004-0840] - Критичная [CVE-2004-0897] - Критичная [CVE-2004-0899] - Средняя [CVE-2004-0900] - Критичная [CVE-2004-0901] - Критичная [CVE-2004-1049] - Средняя [CVE-2004-1080] - Критичная [CVE-2004-1324] - Низкая [CVE-2004-1325] - Средняя [CVE-2004-1889] - Средняя [CVE-2004-2176] - Средняя [CVE-2004-2289] - Критичная [CVE-2004-2290] - Высокая [CVE-2004-2291] - Высокая [CVE-2004-2307] - Средняя [CVE-2004-2339] - Высокая [CVE-2004-2365] - Низкая [CVE-2004-2454] - Низкая [CVE-2004-2527] - Средняя [CVE-2005-0048] - Высокая [CVE-2005-0058] - Высокая [CVE-2005-0059] - Критичная [CVE-2005-0060] - Высокая [CVE-2005-0061] - Высокая [CVE-2005-0063] - Высокая [CVE-2005-0545] - Высокая [CVE-2005-0550] - Низкая [CVE-2005-0551] - Критичная [CVE-2005-0771] - Критичная [CVE-2005-0852] - Низкая [CVE-2005-1205] - Средняя [CVE-2005-1206] - Высокая [CVE-2005-1207] - Высокая [CVE-2005-1208] - Критичная [CVE-2005-1218] - Средняя [CVE-2005-1219] - Высокая [CVE-2005-1792] - Средняя [CVE-2005-1793] - Низкая [CVE-2005-1978] - Высокая [CVE-2005-1979] - Средняя [CVE-2005-1980] - Средняя [CVE-2005-1981] - Низкая [CVE-2005-1982] - Низкая [CVE-2005-1983] - Критичная [CVE-2005-1984] - Высокая [CVE-2005-1985] - Высокая [CVE-2005-1987] - Высокая [CVE-2005-2117] - Средняя [CVE-2005-2118] - Средняя [CVE-2005-2120] - Средняя [CVE-2005-2122] - Критичная [CVE-2005-2128] - Средняя [CVE-2005-2224] - Средняя [CVE-2005-2307] - Средняя [CVE-2005-2388] - Высокая [CVE-2005-2935] - Средняя [CVE-2005-2940] - Высокая [CVE-2005-3168] - Высокая [CVE-2005-3169] - Средняя [CVE-2005-3170] - Средняя [CVE-2005-3171] - Средняя [CVE-2005-3172] - Средняя [CVE-2005-3173] - Средняя [CVE-2005-3174] - Средняя [CVE-2005-3175] - Высокая [CVE-2005-3176] - Высокая [CVE-2005-3177] - Средняя [CVE-2005-3595] - Критичная [CVE-2005-3945] - Высокая [CVE-2005-3981] - Средняя [CVE-2005-4269] - Высокая [CVE-2005-4360] - Высокая [CVE-2005-4560] - Высокая [CVE-2005-4717] - Средняя [CVE-2006-0005] - Критичная [CVE-2006-0006] - Критичная [CVE-2006-0008] - Высокая [CVE-2006-0010] - Критичная [CVE-2006-0012] - Средняя [CVE-2006-0014] - Средняя [CVE-2006-0020] - Критичная [CVE-2006-0021] - Высокая [CVE-2006-0023] - Средняя [CVE-2006-0025] - Критичная [CVE-2006-0032] - Средняя [CVE-2006-0143] - Высокая [CVE-2006-0561] - Высокая [CVE-2006-0753] - Низкая [CVE-2006-0988] - Высокая [CVE-2006-1184] - Средняя [CVE-2006-1300] - Средняя [CVE-2006-1311] - Критичная [CVE-2006-1313] - Средняя [CVE-2006-1314] - Высокая [CVE-2006-1315] - Средняя [CVE-2006-1475] - Низкая [CVE-2006-1476] - Низкая [CVE-2006-1510] - Средняя [CVE-2006-1591] - Средняя [CVE-2006-1651] - Высокая [CVE-2006-1654] - Средняя [CVE-2006-2056] - Средняя [CVE-2006-2094] - Средняя [CVE-2006-2218] - Критичная [CVE-2006-2334] - Низкая [CVE-2006-2372] - Критичная [CVE-2006-2373] - Критичная [CVE-2006-2374] - Низкая [CVE-2006-2376] - Высокая [CVE-2006-2378] - Средняя [CVE-2006-2379] - Критичная [CVE-2006-2386] - Средняя [CVE-2006-2766] - Низкая [CVE-2006-3209] - Высокая [CVE-2006-3440] - Критичная [CVE-2006-3441] - Критичная [CVE-2006-3442] - Высокая [CVE-2006-3443] - Высокая [CVE-2006-3444] - Высокая [CVE-2006-3445] - Высокая [CVE-2006-3448] - Критичная [CVE-2006-3471] - Средняя [CVE-2006-3510] - Низкая [CVE-2006-3643] - Средняя [CVE-2006-3648] - Высокая [CVE-2006-3730] - Критичная [CVE-2006-3869] - Высокая [CVE-2006-3873] - Высокая [CVE-2006-3880] - Средняя [CVE-2006-3897] - Средняя [CVE-2006-3898] - Средняя [CVE-2006-3899] - Средняя [CVE-2006-3915] - Средняя [CVE-2006-3942] - Высокая [CVE-2006-3943] - Низкая [CVE-2006-3944] - Средняя [CVE-2006-3992] - Средняя [CVE-2006-4066] - Низкая [CVE-2006-4071] - Низкая [CVE-2006-4128] - Средняя [CVE-2006-4138] - Высокая [CVE-2006-4219] - Высокая [CVE-2006-4495] - Высокая [CVE-2006-4688] - Высокая [CVE-2006-4689] - Средняя [CVE-2006-4692] - Средняя [CVE-2006-4694] - Критичная [CVE-2006-4696] - Критичная [CVE-2006-4702] - Средняя [CVE-2006-4868] - Критичная [CVE-2006-5028] - Средняя [CVE-2006-5270] - Критичная [CVE-2006-5448] - Высокая [CVE-2006-5583] - Критичная [CVE-2006-5584] - Высокая [CVE-2006-5585] - Высокая [CVE-2006-5586] - Высокая [CVE-2006-5614] - Низкая [CVE-2006-5745] - Высокая [CVE-2006-5758] - Высокая [CVE-2006-6134] - Высокая [CVE-2006-6252] - Средняя [CVE-2006-6579] - Средняя [CVE-2006-6601] - Средняя [CVE-2006-6602] - Средняя [CVE-2006-6659] - Средняя [CVE-2006-6696] - Средняя [CVE-2006-6753] - Средняя [CVE-2006-6797] - Средняя [CVE-2006-6901] - Критичная [CVE-2006-6902] - Критичная [CVE-2006-7066] - Высокая [CVE-2006-7206] - Высокая [CVE-2006-7210] - Средняя [CVE-2007-0024] - Критичная [CVE-2007-0025] - Критичная [CVE-2007-0026] - Высокая [CVE-2007-0038] - Критичная [CVE-2007-0040] - Критичная [CVE-2007-0041] - Критичная [CVE-2007-0042] - Высокая [CVE-2007-0043] - Критичная [CVE-2007-0045] - Средняя [CVE-2007-0064] - Критичная [CVE-2007-0065] - Критичная [CVE-2007-0066] - Высокая [CVE-2007-0069] - Критичная [CVE-2007-0084] - Средняя [CVE-2007-0210] - Высокая [CVE-2007-0211] - Высокая [CVE-2007-0214] - Критичная [CVE-2007-0351] - Средняя [CVE-2007-0562] - Средняя [CVE-2007-0612] - Высокая [CVE-2007-0675] - Высокая [CVE-2007-0811] - Средняя [CVE-2007-0843] - Средняя [CVE-2007-0878] - Высокая [CVE-2007-0942] - Критичная [CVE-2007-0944] - Критичная [CVE-2007-0945] - Критичная [CVE-2007-0946] - Критичная [CVE-2007-0947] - Критичная [CVE-2007-1070] - Критичная [CVE-2007-1090] - Высокая [CVE-2007-1204] - Средняя [CVE-2007-1205] - Критичная [CVE-2007-1206] - Высокая [CVE-2007-1209] - Высокая [CVE-2007-1211] - Высокая [CVE-2007-1212] - Средняя [CVE-2007-1213] - Высокая [CVE-2007-1215] - Высокая [CVE-2007-1347] - Высокая [CVE-2007-1492] - Высокая [CVE-2007-1499] - Средняя [CVE-2007-1512] - Критичная [CVE-2007-1527] - Средняя [CVE-2007-1528] - Средняя [CVE-2007-1529] - Средняя [CVE-2007-1530] - Средняя [CVE-2007-1531] - Средняя [CVE-2007-1532] - Средняя [CVE-2007-1533] - Средняя [CVE-2007-1534] - Критичная [CVE-2007-1535] - Высокая [CVE-2007-1537] - Низкая [CVE-2007-1644] - Критичная [CVE-2007-1645] - Критичная [CVE-2007-1658] - Критичная [CVE-2007-1692] - Высокая [CVE-2007-1763] - Высокая [CVE-2007-1765] - Критичная [CVE-2007-1912] - Средняя [CVE-2007-1946] - Критичная [CVE-2007-1973] - Средняя [CVE-2007-2217] - Критичная [CVE-2007-2218] - Критичная [CVE-2007-2219] - Критичная [CVE-2007-2221] - Критичная [CVE-2007-2224] - Критичная [CVE-2007-2225] - Средняя [CVE-2007-2227] - Средняя [CVE-2007-2229] - Высокая [CVE-2007-2237] - Высокая [CVE-2007-2374] - Критичная [CVE-2007-2528] - Критичная [CVE-2007-2581] - Средняя [CVE-2007-2593] - Высокая [CVE-2007-2729] - Высокая [CVE-2007-2730] - Высокая [CVE-2007-2815] - Критичная [CVE-2007-2954] - Критичная [CVE-2007-2966] - Высокая [CVE-2007-2967] - Критичная [CVE-2007-2999] - Низкая [CVE-2007-3028] - Средняя [CVE-2007-3034] - Критичная [CVE-2007-3035] - Высокая [CVE-2007-3036] - Средняя [CVE-2007-3037] - Средняя [CVE-2007-3038] - Высокая [CVE-2007-3040] - Критичная [CVE-2007-3300] - Критичная [CVE-2007-3406] - Средняя [CVE-2007-3436] - Средняя [CVE-2007-3463] - Средняя [CVE-2007-3509] - Высокая [CVE-2007-3671] - Высокая [CVE-2007-3724] - Низкая [CVE-2007-3826] - Критичная [CVE-2007-3896] - Критичная [CVE-2007-3897] - Критичная [CVE-2007-3898] - Средняя [CVE-2007-3958] - Высокая [CVE-2007-4218] - Критичная [CVE-2007-4219] - Критичная [CVE-2007-4227] - Средняя [CVE-2007-4247] - Средняя [CVE-2007-4288] - Средняя [CVE-2007-4414] - Средняя [CVE-2007-4490] - Критичная [CVE-2007-5095] - Высокая [CVE-2007-5133] - Высокая [CVE-2007-5145] - Средняя [CVE-2007-5348] - Критичная [CVE-2007-5350] - Высокая [CVE-2007-5351] - Критичная [CVE-2007-5352] - Высокая [CVE-2007-5460] - Высокая [CVE-2007-5587] - Средняя [CVE-2007-5633] - Высокая [CVE-2007-5634] - Средняя [CVE-2007-6043] - Высокая [CVE-2007-6236] - Средняя [CVE-2007-6332] - Критичная [CVE-2007-6401] - Критичная [CVE-2007-6507] - Критичная [CVE-2007-6701] - Критичная [CVE-2007-6753] - Средняя [CVE-2008-0015] - Критичная [CVE-2008-0020] - Критичная [CVE-2008-0080] - Критичная [CVE-2008-0083] - Критичная [CVE-2008-0084] - Высокая [CVE-2008-0087] - Высокая [CVE-2008-0088] - Средняя [CVE-2008-0322] - Высокая [CVE-2008-0639] - Критичная [CVE-2008-0768] - Критичная [CVE-2008-0951] - Критичная [CVE-2008-1083] - Критичная [CVE-2008-1084] - Высокая [CVE-2008-1086] - Критичная [CVE-2008-1087] - Критичная [CVE-2008-1435] - Критичная [CVE-2008-1436] - Критичная [CVE-2008-1440] - Высокая [CVE-2008-1441] - Средняя [CVE-2008-1444] - Критичная [CVE-2008-1445] - Высокая [CVE-2008-1446] - Критичная [CVE-2008-1448] - Высокая [CVE-2008-1451] - Высокая [CVE-2008-1453] - Высокая [CVE-2008-1454] - Критичная [CVE-2008-1456] - Критичная [CVE-2008-1457] - Критичная [CVE-2008-1888] - Средняя [CVE-2008-2160] - Критичная [CVE-2008-2245] - Критичная [CVE-2008-2246] - Высокая [CVE-2008-2249] - Критичная [CVE-2008-2250] - Высокая [CVE-2008-2251] - Высокая [CVE-2008-2252] - Высокая [CVE-2008-2253] - Критичная [CVE-2008-2540] - Критичная [CVE-2008-2547] - Критичная [CVE-2008-3008] - Критичная [CVE-2008-3009] - Критичная [CVE-2008-3010] - Критичная [CVE-2008-3012] - Критичная [CVE-2008-3013] - Критичная [CVE-2008-3014] - Критичная [CVE-2008-3068] - Высокая [CVE-2008-3464] - Высокая [CVE-2008-3465] - Критичная [CVE-2008-3466] - Критичная [CVE-2008-3636] - Высокая [CVE-2008-3648] - Критичная [CVE-2008-3815] - Средняя [CVE-2008-3893] - Низкая [CVE-2008-3957] - Критичная [CVE-2008-4023] - Критичная [CVE-2008-4036] - Высокая [CVE-2008-4037] - Критичная [CVE-2008-4038] - Критичная [CVE-2008-4071] - Средняя [CVE-2008-4127] - Средняя [CVE-2008-4255] - Критичная [CVE-2008-4261] - Критичная [CVE-2008-4268] - Высокая [CVE-2008-4269] - Высокая [CVE-2008-4295] - Средняя [CVE-2008-4323] - Средняя [CVE-2008-4327] - Средняя [CVE-2008-4510] - Средняя [CVE-2008-4609] - Высокая [CVE-2008-4834] - Критичная [CVE-2008-4835] - Критичная [CVE-2008-4841] - Критичная [CVE-2008-4927] - Средняя [CVE-2008-5044] - Средняя [CVE-2008-5112] - Средняя [CVE-2008-5179] - Средняя [CVE-2008-5229] - Средняя [CVE-2008-5232] - Критичная [CVE-2008-5415] - Критичная [CVE-2008-5745] - Средняя [CVE-2008-5750] - Средняя [CVE-2008-5823] - Средняя [CVE-2008-5828] - Средняя [CVE-2008-6194] - Высокая [CVE-2008-6219] - Высокая [CVE-2008-6819] - Средняя [CVE-2009-0078] - Высокая [CVE-2009-0081] - Критичная [CVE-2009-0082] - Высокая [CVE-2009-0083] - Высокая [CVE-2009-0085] - Высокая [CVE-2009-0086] - Критичная [CVE-2009-0087] - Критичная [CVE-2009-0089] - Средняя [CVE-2009-0093] - Низкая [CVE-2009-0094] - Средняя [CVE-2009-0119] - Критичная [CVE-2009-0202] - Критичная [CVE-2009-0229] - Средняя [CVE-2009-0231] - Критичная [CVE-2009-0232] - Критичная [CVE-2009-0233] - Средняя [CVE-2009-0234] - Средняя [CVE-2009-0235] - Критичная [CVE-2009-0239] - Средняя [CVE-2009-0243] - Высокая [CVE-2009-0244] - Высокая [CVE-2009-0320] - Средняя [CVE-2009-0341] - Критичная [CVE-2009-0550] - Критичная [CVE-2009-0551] - Критичная [CVE-2009-0552] - Критичная [CVE-2009-0553] - Критичная [CVE-2009-0554] - Критичная [CVE-2009-0555] - Критичная [CVE-2009-1043] - Критичная [CVE-2009-1122] - Высокая [CVE-2009-1123] - Высокая [CVE-2009-1124] - Высокая [CVE-2009-1125] - Высокая [CVE-2009-1126] - Высокая [CVE-2009-1127] - Высокая [CVE-2009-1132] - Критичная [CVE-2009-1133] - Критичная [CVE-2009-1138] - Критичная [CVE-2009-1139] - Высокая [CVE-2009-1141] - Критичная [CVE-2009-1216] - Критичная [CVE-2009-1217] - Средняя [CVE-2009-1331] - Критичная [CVE-2009-1335] - Средняя [CVE-2009-1511] - Высокая [CVE-2009-1528] - Критичная [CVE-2009-1529] - Критичная [CVE-2009-1530] - Критичная [CVE-2009-1531] - Критичная [CVE-2009-1532] - Критичная [CVE-2009-1533] - Критичная [CVE-2009-1537] - Критичная [CVE-2009-1538] - Критичная [CVE-2009-1539] - Критичная [CVE-2009-1545] - Критичная [CVE-2009-1546] - Высокая [CVE-2009-1761] - Средняя [CVE-2009-1808] - Средняя [CVE-2009-1920] - Критичная [CVE-2009-1922] - Средняя [CVE-2009-1923] - Критичная [CVE-2009-1924] - Критичная [CVE-2009-1925] - Критичная [CVE-2009-1926] - Высокая [CVE-2009-1928] - Высокая [CVE-2009-1929] - Критичная [CVE-2009-1930] - Критичная [CVE-2009-2357] - Критичная [CVE-2009-2484] - Критичная [CVE-2009-2494] - Критичная [CVE-2009-2498] - Критичная [CVE-2009-2499] - Высокая [CVE-2009-2500] - Критичная [CVE-2009-2501] - Критичная [CVE-2009-2502] - Критичная [CVE-2009-2503] - Критичная [CVE-2009-2504] - Критичная [CVE-2009-2505] - Критичная [CVE-2009-2507] - Критичная [CVE-2009-2508] - Средняя [CVE-2009-2509] - Критичная [CVE-2009-2510] - Средняя [CVE-2009-2511] - Высокая [CVE-2009-2513] - Высокая [CVE-2009-2514] - Критичная [CVE-2009-2515] - Высокая [CVE-2009-2516] - Средняя [CVE-2009-2517] - Средняя [CVE-2009-2519] - Критичная [CVE-2009-2524] - Высокая [CVE-2009-2525] - Критичная [CVE-2009-2526] - Высокая [CVE-2009-2527] - Критичная [CVE-2009-2532] - Критичная [CVE-2009-2544] - Средняя [CVE-2009-2653] - Средняя [CVE-2009-2655] - Средняя [CVE-2009-2764] - Средняя [CVE-2009-3019] - Средняя [CVE-2009-3020] - Высокая [CVE-2009-3103] - Критичная [CVE-2009-3126] - Критичная [CVE-2009-3294] - Средняя [CVE-2009-3675] - Средняя [CVE-2009-3676] - Высокая [CVE-2009-3677] - Критичная [CVE-2009-3678] - Критичная [CVE-2009-4210] - Критичная [CVE-2009-4309] - Критичная [CVE-2009-4310] - Критичная [CVE-2009-4311] - Критичная [CVE-2009-4312] - Критичная [CVE-2009-4313] - Критичная [CVE-2010-0016] - Критичная [CVE-2010-0017] - Критичная [CVE-2010-0018] - Критичная [CVE-2010-0019] - Критичная [CVE-2010-0020] - Критичная [CVE-2010-0021] - Высокая [CVE-2010-0022] - Высокая [CVE-2010-0023] - Средняя [CVE-2010-0024] - Средняя [CVE-2010-0025] - Средняя [CVE-2010-0026] - Средняя [CVE-2010-0027] - Критичная [CVE-2010-0028] - Критичная [CVE-2010-0035] - Средняя [CVE-2010-0231] - Критичная [CVE-2010-0232] - Высокая [CVE-2010-0233] - Высокая [CVE-2010-0234] - Средняя [CVE-2010-0235] - Средняя [CVE-2010-0236] - Высокая [CVE-2010-0237] - Средняя [CVE-2010-0238] - Средняя [CVE-2010-0239] - Критичная [CVE-2010-0240] - Критичная [CVE-2010-0241] - Критичная [CVE-2010-0242] - Высокая [CVE-2010-0249] - Критичная [CVE-2010-0250] - Критичная [CVE-2010-0252] - Критичная [CVE-2010-0265] - Критичная [CVE-2010-0268] - Критичная [CVE-2010-0269] - Критичная [CVE-2010-0270] - Критичная [CVE-2010-0278] - Средняя [CVE-2010-0378] - Критичная [CVE-2010-0379] - Критичная [CVE-2010-0476] - Критичная [CVE-2010-0477] - Критичная [CVE-2010-0478] - Критичная [CVE-2010-0480] - Критичная [CVE-2010-0481] - Средняя [CVE-2010-0482] - Средняя [CVE-2010-0483] - Высокая [CVE-2010-0484] - Средняя [CVE-2010-0485] - Средняя [CVE-2010-0486] - Критичная [CVE-2010-0487] - Критичная [CVE-2010-0718] - Средняя [CVE-2010-0719] - Средняя [CVE-2010-0805] - Критичная [CVE-2010-0808] - Низкая [CVE-2010-0810] - Средняя [CVE-2010-0811] - Критичная [CVE-2010-0812] - Средняя [CVE-2010-0818] - Критичная [CVE-2010-0819] - Высокая [CVE-2010-0820] - Критичная [CVE-2010-0917] - Высокая [CVE-2010-1042] - Средняя [CVE-2010-1098] - Высокая [CVE-2010-1117] - Высокая [CVE-2010-1118] - Критичная [CVE-2010-1175] - Критичная [CVE-2010-1225] - Критичная [CVE-2010-1255] - Средняя [CVE-2010-1263] - Критичная [CVE-2010-1264] - Средняя [CVE-2010-1689] - Средняя [CVE-2010-1690] - Средняя [CVE-2010-1734] - Средняя [CVE-2010-1735] - Средняя [CVE-2010-1880] - Критичная [CVE-2010-1882] - Критичная [CVE-2010-1883] - Критичная [CVE-2010-1885] - Критичная [CVE-2010-1886] - Средняя [CVE-2010-1887] - Средняя [CVE-2010-1888] - Средняя [CVE-2010-1889] - Высокая [CVE-2010-1890] - Средняя [CVE-2010-1891] - Средняя [CVE-2010-1892] - Высокая [CVE-2010-1893] - Средняя [CVE-2010-1894] - Высокая [CVE-2010-1895] - Высокая [CVE-2010-1896] - Высокая [CVE-2010-1897] - Высокая [CVE-2010-1898] - Критичная [CVE-2010-2091] - Средняя [CVE-2010-2265] - Средняя [CVE-2010-2549] - Высокая [CVE-2010-2550] - Критичная [CVE-2010-2551] - Высокая [CVE-2010-2552] - Высокая [CVE-2010-2553] - Критичная [CVE-2010-2554] - Средняя [CVE-2010-2555] - Средняя [CVE-2010-2563] - Критичная [CVE-2010-2564] - Критичная [CVE-2010-2566] - Критичная [CVE-2010-2568] - Критичная [CVE-2010-2731] - Средняя [CVE-2010-2738] - Критичная [CVE-2010-2739] - Высокая [CVE-2010-2740] - Высокая [CVE-2010-2741] - Высокая [CVE-2010-2743] - Высокая [CVE-2010-2744] - Высокая [CVE-2010-2745] - Критичная [CVE-2010-2746] - Высокая [CVE-2010-3138] - Критичная [CVE-2010-3140] - Критичная [CVE-2010-3143] - Критичная [CVE-2010-3144] - Критичная [CVE-2010-3145] - Критичная [CVE-2010-3147] - Критичная [CVE-2010-3223] - Высокая [CVE-2010-3225] - Высокая [CVE-2010-3227] - Критичная [CVE-2010-3229] - Высокая [CVE-2010-3243] - Средняя [CVE-2010-3324] - Средняя [CVE-2010-3338] - Высокая [CVE-2010-3888] - Высокая [CVE-2010-3889] - Высокая [CVE-2010-3937] - Средняя [CVE-2010-3939] - Высокая [CVE-2010-3940] - Высокая [CVE-2010-3941] - Высокая [CVE-2010-3942] - Высокая [CVE-2010-3943] - Высокая [CVE-2010-3944] - Высокая [CVE-2010-3956] - Критичная [CVE-2010-3957] - Средняя [CVE-2010-3959] - Средняя [CVE-2010-3960] - Средняя [CVE-2010-3961] - Высокая [CVE-2010-3963] - Высокая [CVE-2010-3965] - Критичная [CVE-2010-3966] - Критичная [CVE-2010-3967] - Критичная [CVE-2010-3970] - Критичная [CVE-2010-3973] - Критичная [CVE-2010-3974] - Высокая [CVE-2010-4182] - Критичная [CVE-2010-4398] - Высокая [CVE-2010-4562] - Средняя [CVE-2010-4669] - Высокая [CVE-2010-4701] - Высокая [CVE-2010-5082] - Критичная [CVE-2011-0026] - Критичная [CVE-2011-0027] - Критичная [CVE-2011-0028] - Критичная [CVE-2011-0030] - Средняя [CVE-2011-0031] - Средняя [CVE-2011-0032] - Критичная [CVE-2011-0033] - Критичная [CVE-2011-0034] - Критичная [CVE-2011-0037] - Высокая [CVE-2011-0039] - Высокая [CVE-2011-0040] - Средняя [CVE-2011-0041] - Критичная [CVE-2011-0042] - Критичная [CVE-2011-0043] - Высокая [CVE-2011-0045] - Высокая [CVE-2011-0086] - Высокая [CVE-2011-0087] - Высокая [CVE-2011-0088] - Высокая [CVE-2011-0089] - Высокая [CVE-2011-0090] - Высокая [CVE-2011-0091] - Средняя [CVE-2011-0096] - Средняя [CVE-2011-0347] - Критичная [CVE-2011-0627] - Критичная [CVE-2011-0638] - Средняя [CVE-2011-0654] - Критичная [CVE-2011-0657] - Высокая [CVE-2011-0658] - Критичная [CVE-2011-0660] - Критичная [CVE-2011-0661] - Критичная [CVE-2011-0662] - Высокая [CVE-2011-0665] - Высокая [CVE-2011-0666] - Высокая [CVE-2011-0667] - Высокая [CVE-2011-0670] - Высокая [CVE-2011-0671] - Высокая [CVE-2011-0672] - Высокая [CVE-2011-0673] - Высокая [CVE-2011-0674] - Высокая [CVE-2011-0675] - Высокая [CVE-2011-0676] - Высокая [CVE-2011-0677] - Высокая [CVE-2011-1068] - Низкая [CVE-2011-1225] - Высокая [CVE-2011-1226] - Высокая [CVE-2011-1227] - Высокая [CVE-2011-1228] - Высокая [CVE-2011-1229] - Высокая [CVE-2011-1230] - Высокая [CVE-2011-1231] - Высокая [CVE-2011-1232] - Высокая [CVE-2011-1233] - Высокая [CVE-2011-1234] - Высокая [CVE-2011-1235] - Высокая [CVE-2011-1236] - Высокая [CVE-2011-1237] - Высокая [CVE-2011-1238] - Высокая [CVE-2011-1239] - Высокая [CVE-2011-1240] - Высокая [CVE-2011-1241] - Высокая [CVE-2011-1242] - Высокая [CVE-2011-1243] - Критичная [CVE-2011-1247] - Критичная [CVE-2011-1248] - Критичная [CVE-2011-1249] - Высокая [CVE-2011-1252] - Средняя [CVE-2011-1263] - Средняя [CVE-2011-1264] - Средняя [CVE-2011-1265] - Высокая [CVE-2011-1267] - Высокая [CVE-2011-1268] - Критичная [CVE-2011-1281] - Высокая [CVE-2011-1282] - Высокая [CVE-2011-1283] - Высокая [CVE-2011-1284] - Высокая [CVE-2011-1346] - Критичная [CVE-2011-1347] - Высокая [CVE-2011-1652] - Средняя [CVE-2011-1713] - Средняя [CVE-2011-1868] - Критичная [CVE-2011-1869] - Высокая [CVE-2011-1870] - Высокая [CVE-2011-1871] - Высокая [CVE-2011-1872] - Средняя [CVE-2011-1873] - Критичная [CVE-2011-1874] - Высокая [CVE-2011-1875] - Высокая [CVE-2011-1876] - Высокая [CVE-2011-1877] - Высокая [CVE-2011-1878] - Высокая [CVE-2011-1879] - Высокая [CVE-2011-1880] - Высокая [CVE-2011-1881] - Высокая [CVE-2011-1882] - Высокая [CVE-2011-1883] - Высокая [CVE-2011-1884] - Высокая [CVE-2011-1885] - Высокая [CVE-2011-1886] - Низкая [CVE-2011-1887] - Высокая [CVE-2011-1888] - Высокая [CVE-2011-1891] - Средняя [CVE-2011-1892] - Средняя [CVE-2011-1893] - Средняя [CVE-2011-1894] - Средняя [CVE-2011-1965] - Высокая [CVE-2011-1966] - Критичная [CVE-2011-1967] - Высокая [CVE-2011-1968] - Высокая [CVE-2011-1970] - Средняя [CVE-2011-1971] - Средняя [CVE-2011-1974] - Высокая [CVE-2011-1975] - Критичная [CVE-2011-1984] - Высокая [CVE-2011-1985] - Высокая [CVE-2011-1991] - Критичная [CVE-2011-2002] - Средняя [CVE-2011-2003] - Критичная [CVE-2011-2004] - Высокая [CVE-2011-2005] - Высокая [CVE-2011-2009] - Критичная [CVE-2011-2011] - Высокая [CVE-2011-2013] - Критичная [CVE-2011-2014] - Критичная [CVE-2011-2016] - Критичная [CVE-2011-2018] - Высокая [CVE-2011-2019] - Критичная [CVE-2011-3389] - Средняя [CVE-2011-3397] - Критичная [CVE-2011-3400] - Критичная [CVE-2011-3401] - Критичная [CVE-2011-3402] - Критичная [CVE-2011-3406] - Критичная [CVE-2011-3408] - Высокая [CVE-2011-4434] - Низкая [CVE-2011-4695] - Средняя [CVE-2011-5046] - Критичная [CVE-2011-5279] - Средняя [CVE-2012-0001] - Критичная [CVE-2012-0002] - Критичная [CVE-2012-0003] - Критичная [CVE-2012-0004] - Критичная [CVE-2012-0005] - Средняя [CVE-2012-0006] - Средняя [CVE-2012-0009] - Критичная [CVE-2012-0013] - Критичная [CVE-2012-0148] - Высокая [CVE-2012-0149] - Высокая [CVE-2012-0150] - Критичная [CVE-2012-0151] - Критичная [CVE-2012-0152] - Средняя [CVE-2012-0154] - Высокая [CVE-2012-0156] - Средняя [CVE-2012-0157] - Высокая [CVE-2012-0159] - Критичная [CVE-2012-0164] - Средняя [CVE-2012-0165] - Критичная [CVE-2012-0173] - Критичная [CVE-2012-0174] - Низкая [CVE-2012-0175] - Критичная [CVE-2012-0176] - Критичная [CVE-2012-0178] - Высокая [CVE-2012-0179] - Высокая [CVE-2012-0180] - Высокая [CVE-2012-0181] - Высокая [CVE-2012-1194] - Средняя [CVE-2012-1527] - Критичная [CVE-2012-1528] - Критичная [CVE-2012-1537] - Критичная [CVE-2012-1848] - Высокая [CVE-2012-1850] - Средняя [CVE-2012-1851] - Критичная [CVE-2012-1852] - Критичная [CVE-2012-1853] - Критичная [CVE-2012-1863] - Средняя [CVE-2012-1864] - Высокая [CVE-2012-1865] - Высокая [CVE-2012-1866] - Высокая [CVE-2012-1867] - Высокая [CVE-2012-1868] - Средняя [CVE-2012-1870] - Средняя [CVE-2012-1890] - Высокая [CVE-2012-1891] - Критичная [CVE-2012-1893] - Высокая [CVE-2012-1945] - Низкая [CVE-2012-2520] - Средняя [CVE-2012-2526] - Критичная [CVE-2012-2527] - Высокая [CVE-2012-2529] - Высокая [CVE-2012-2530] - Высокая [CVE-2012-2551] - Средняя [CVE-2012-2553] - Высокая [CVE-2012-2556] - Критичная [CVE-2012-2897] - Критичная [CVE-2012-2971] - Высокая [CVE-2012-2972] - Средняя [CVE-2012-2993] - Низкая [CVE-2012-4774] - Критичная [CVE-2012-4786] - Критичная [CVE-2012-5362] - Высокая [CVE-2012-5364] - Высокая [CVE-2013-0001] - Средняя [CVE-2013-0002] - Критичная [CVE-2013-0005] - Высокая [CVE-2013-0008] - Высокая [CVE-2013-0011] - Критичная [CVE-2013-0013] - Средняя [CVE-2013-0073] - Критичная [CVE-2013-0075] - Высокая [CVE-2013-0076] - Высокая [CVE-2013-0077] - Критичная [CVE-2013-0078] - Высокая [CVE-2013-0096] - Средняя [CVE-2013-0810] - Критичная [CVE-2013-0941] - Низкая [CVE-2013-1248] - Средняя [CVE-2013-1249] - Средняя [CVE-2013-1250] - Средняя [CVE-2013-1251] - Средняя [CVE-2013-1252] - Средняя [CVE-2013-1253] - Средняя [CVE-2013-1254] - Средняя [CVE-2013-1255] - Средняя [CVE-2013-1256] - Средняя [CVE-2013-1257] - Средняя [CVE-2013-1258] - Средняя [CVE-2013-1259] - Средняя [CVE-2013-1260] - Средняя [CVE-2013-1261] - Средняя [CVE-2013-1262] - Средняя [CVE-2013-1263] - Средняя [CVE-2013-1264] - Средняя [CVE-2013-1265] - Средняя [CVE-2013-1266] - Средняя [CVE-2013-1267] - Средняя [CVE-2013-1268] - Средняя [CVE-2013-1269] - Средняя [CVE-2013-1270] - Средняя [CVE-2013-1271] - Средняя [CVE-2013-1272] - Средняя [CVE-2013-1273] - Средняя [CVE-2013-1274] - Средняя [CVE-2013-1275] - Средняя [CVE-2013-1276] - Средняя [CVE-2013-1277] - Средняя [CVE-2013-1278] - Высокая [CVE-2013-1279] - Высокая [CVE-2013-1280] - Высокая [CVE-2013-1281] - Высокая [CVE-2013-1283] - Средняя [CVE-2013-1284] - Средняя [CVE-2013-1285] - Высокая [CVE-2013-1286] - Высокая [CVE-2013-1287] - Высокая [CVE-2013-1291] - Высокая [CVE-2013-1292] - Средняя [CVE-2013-1293] - Средняя [CVE-2013-1294] - Средняя [CVE-2013-1295] - Высокая [CVE-2013-1299] - Средняя [CVE-2013-1300] - Высокая [CVE-2013-1305] - Высокая [CVE-2013-1313] - Критичная [CVE-2013-1332] - Высокая [CVE-2013-1333] - Высокая [CVE-2013-1334] - Высокая [CVE-2013-1337] - Высокая [CVE-2013-1339] - Критичная [CVE-2013-1340] - Высокая [CVE-2013-1341] - Высокая [CVE-2013-1342] - Высокая [CVE-2013-1343] - Высокая [CVE-2013-1344] - Высокая [CVE-2013-1345] - Высокая [CVE-2013-2552] - Высокая [CVE-2013-2553] - Высокая [CVE-2013-2554] - Высокая [CVE-2013-2556] - Высокая [CVE-2013-2558] - Критичная [CVE-2013-3127] - Критичная [CVE-2013-3128] - Критичная [CVE-2013-3136] - Средняя [CVE-2013-3138] - Высокая [CVE-2013-3154] - Средняя [CVE-2013-3167] - Высокая [CVE-2013-3172] - Средняя [CVE-2013-3173] - Высокая [CVE-2013-3174] - Критичная [CVE-2013-3181] - Критичная [CVE-2013-3182] - Высокая [CVE-2013-3183] - Высокая [CVE-2013-3185] - Средняя [CVE-2013-3186] - Высокая [CVE-2013-3195] - Критичная [CVE-2013-3196] - Высокая [CVE-2013-3197] - Высокая [CVE-2013-3198] - Высокая [CVE-2013-3200] - Высокая [CVE-2013-3660] - Средняя [CVE-2013-3661] - Средняя [CVE-2013-3862] - Средняя [CVE-2013-3863] - Критичная [CVE-2013-3864] - Высокая [CVE-2013-3865] - Высокая [CVE-2013-3866] - Высокая [CVE-2013-3868] - Средняя [CVE-2013-3869] - Средняя [CVE-2013-3876] - Высокая [CVE-2013-3879] - Высокая [CVE-2013-3880] - Низкая [CVE-2013-3881] - Высокая [CVE-2013-3887] - Средняя [CVE-2013-3888] - Высокая [CVE-2013-3894] - Критичная [CVE-2013-3898] - Высокая [CVE-2013-3899] - Высокая [CVE-2013-3900] - Высокая [CVE-2013-3902] - Высокая [CVE-2013-3903] - Средняя [CVE-2013-3906] - Критичная [CVE-2013-3907] - Высокая [CVE-2013-3918] - Критичная [CVE-2013-3940] - Критичная [CVE-2013-4858] - Средняя [CVE-2013-5056] - Критичная [CVE-2013-5058] - Средняя [CVE-2013-5065] - Высокая [CVE-2013-6230] - Средняя [CVE-2013-6801] - Высокая [CVE-2013-6999] - Средняя [CVE-2013-7331] - Средняя [CVE-2013-7332] - Средняя [CVE-2013-7369] - Высокая [CVE-2014-0251] - Критичная [CVE-2014-0254] - Высокая [CVE-2014-0255] - Средняя [CVE-2014-0256] - Средняя [CVE-2014-0262] - Высокая [CVE-2014-0263] - Критичная [CVE-2014-0266] - Высокая [CVE-2014-0296] - Средняя [CVE-2014-0300] - Высокая [CVE-2014-0301] - Критичная [CVE-2014-0315] - Средняя [CVE-2014-0317] - Средняя [CVE-2014-0318] - Высокая [CVE-2014-0323] - Средняя [CVE-2014-1767] - Высокая [CVE-2014-1807] - Высокая [CVE-2014-1811] - Средняя [CVE-2014-1812] - Критичная [CVE-2014-1814] - Высокая [CVE-2014-1817] - Критичная [CVE-2014-1818] - Критичная [CVE-2014-1819] - Высокая [CVE-2014-1824] - Критичная [CVE-2014-2671] - Средняя [CVE-2014-2780] - Средняя [CVE-2014-2781] - Высокая [CVE-2014-2814] - Средняя [CVE-2014-4060] - Средняя [CVE-2014-4064] - Средняя [CVE-2014-4074] - Высокая [CVE-2014-4076] - Высокая [CVE-2014-4077] - Критичная [CVE-2014-4113] - Высокая [CVE-2014-4114] - Критичная [CVE-2014-4115] - Высокая [CVE-2014-4118] - Критичная [CVE-2014-4148] - Критичная [CVE-2014-4971] - Высокая [CVE-2014-6317] - Высокая [CVE-2014-6318] - Средняя [CVE-2014-6321] - Критичная [CVE-2014-6322] - Средняя [CVE-2014-6324] - Критичная [CVE-2014-6332] - Критичная [CVE-2014-6352] - Критичная [CVE-2014-6355] - Средняя [CVE-2015-0001] - Низкая [CVE-2015-0002] - Высокая [CVE-2015-0003] - Средняя [CVE-2015-0004] - Высокая [CVE-2015-0005] - Средняя [CVE-2015-0006] - Средняя [CVE-2015-0008] - Высокая [CVE-2015-0009] - Низкая [CVE-2015-0010] - Низкая [CVE-2015-0011] - Средняя [CVE-2015-0014] - Критичная [CVE-2015-0015] - Высокая [CVE-2015-0016] - Критичная [CVE-2015-0057] - Высокая [CVE-2015-0058] - Высокая [CVE-2015-0059] - Средняя [CVE-2015-0060] - Средняя [CVE-2015-0061] - Средняя [CVE-2015-0062] - Высокая [CVE-2015-0073] - Высокая [CVE-2015-0074] - Средняя [CVE-2015-0075] - Высокая [CVE-2015-0076] - Средняя [CVE-2015-0077] - Низкая [CVE-2015-0078] - Высокая [CVE-2015-0079] - Высокая [CVE-2015-0080] - Средняя [CVE-2015-0081] - Критичная [CVE-2015-0084] - Низкая [CVE-2015-0085] - Критичная [CVE-2015-0087] - Средняя [CVE-2015-0088] - Критичная [CVE-2015-0089] - Средняя [CVE-2015-0090] - Критичная [CVE-2015-0091] - Критичная [CVE-2015-0092] - Критичная [CVE-2015-0093] - Критичная [CVE-2015-0094] - Низкая [CVE-2015-0095] - Средняя [CVE-2015-0096] - Критичная [CVE-2015-0098] - Высокая [CVE-2015-1635] - Критичная [CVE-2015-1637] - Средняя [CVE-2015-1638] - Средняя [CVE-2015-1643] - Высокая [CVE-2015-1644] - Высокая [CVE-2015-1645] - Критичная [CVE-2015-1647] - Низкая [CVE-2015-1670] - Средняя [CVE-2015-1671] - Критичная [CVE-2015-1673] - Критичная [CVE-2015-1674] - Средняя [CVE-2015-1675] - Критичная [CVE-2015-1676] - Низкая [CVE-2015-1677] - Низкая [CVE-2015-1678] - Низкая [CVE-2015-1679] - Низкая [CVE-2015-1680] - Низкая [CVE-2015-1681] - Низкая [CVE-2015-1695] - Критичная [CVE-2015-1696] - Критичная [CVE-2015-1697] - Критичная [CVE-2015-1698] - Критичная [CVE-2015-1699] - Критичная [CVE-2015-1701] - Высокая [CVE-2015-1702] - Средняя [CVE-2015-1716] - Средняя [CVE-2015-1719] - Низкая [CVE-2015-1720] - Высокая [CVE-2015-1721] - Высокая [CVE-2015-1722] - Высокая [CVE-2015-1723] - Высокая [CVE-2015-1724] - Высокая [CVE-2015-1725] - Высокая [CVE-2015-1726] - Высокая [CVE-2015-1727] - Высокая [CVE-2015-1728] - Критичная [CVE-2015-1756] - Критичная [CVE-2015-1757] - Средняя [CVE-2015-1758] - Средняя [CVE-2015-1768] - Высокая [CVE-2015-1769] - Высокая [CVE-2015-2360] - Высокая [CVE-2015-2361] - Высокая [CVE-2015-2362] - Высокая [CVE-2015-2363] - Высокая [CVE-2015-2364] - Высокая [CVE-2015-2365] - Высокая [CVE-2015-2366] - Высокая [CVE-2015-2367] - Низкая [CVE-2015-2368] - Средняя [CVE-2015-2369] - Средняя [CVE-2015-2371] - Средняя [CVE-2015-2373] - Критичная [CVE-2015-2374] - Низкая [CVE-2015-2381] - Низкая [CVE-2015-2382] - Низкая [CVE-2015-2387] - Высокая [CVE-2015-2416] - Средняя [CVE-2015-2417] - Средняя [CVE-2015-2423] - Средняя [CVE-2015-2426] - Критичная [CVE-2015-2428] - Низкая [CVE-2015-2429] - Критичная [CVE-2015-2430] - Критичная [CVE-2015-2432] - Критичная [CVE-2015-2433] - Низкая [CVE-2015-2435] - Критичная [CVE-2015-2453] - Средняя [CVE-2015-2454] - Низкая [CVE-2015-2455] - Критичная [CVE-2015-2456] - Критичная [CVE-2015-2458] - Критичная [CVE-2015-2459] - Критичная [CVE-2015-2460] - Критичная [CVE-2015-2461] - Критичная [CVE-2015-2462] - Критичная [CVE-2015-2463] - Критичная [CVE-2015-2464] - Критичная [CVE-2015-2465] - Низкая [CVE-2015-2472] - Средняя [CVE-2015-2473] - Критичная [CVE-2015-2474] - Критичная [CVE-2015-2475] - Средняя [CVE-2015-2476] - Низкая [CVE-2015-2478] - Высокая [CVE-2015-2506] - Критичная [CVE-2015-2507] - Высокая [CVE-2015-2508] - Высокая [CVE-2015-2509] - Критичная [CVE-2015-2510] - Критичная [CVE-2015-2511] - Средняя [CVE-2015-2512] - Высокая [CVE-2015-2513] - Критичная [CVE-2015-2514] - Критичная [CVE-2015-2515] - Критичная [CVE-2015-2516] - Средняя [CVE-2015-2517] - Средняя [CVE-2015-2518] - Средняя [CVE-2015-2519] - Критичная [CVE-2015-2524] - Высокая [CVE-2015-2525] - Высокая [CVE-2015-2527] - Высокая [CVE-2015-2528] - Высокая [CVE-2015-2529] - Низкая [CVE-2015-2530] - Критичная [CVE-2015-2534] - Низкая [CVE-2015-2535] - Средняя [CVE-2015-2546] - Средняя [CVE-2015-2548] - Критичная [CVE-2015-2549] - Высокая [CVE-2015-2550] - Высокая [CVE-2015-2552] - Высокая [CVE-2015-2553] - Высокая [CVE-2015-2554] - Высокая [CVE-2015-4949] - Низкая [CVE-2015-6095] - Средняя [CVE-2015-6097] - Критичная [CVE-2015-6098] - Высокая [CVE-2015-6100] - Средняя [CVE-2015-6101] - Средняя [CVE-2015-6102] - Низкая [CVE-2015-6103] - Критичная [CVE-2015-6104] - Критичная [CVE-2015-6106] - Критичная [CVE-2015-6107] - Критичная [CVE-2015-6108] - Критичная [CVE-2015-6109] - Низкая [CVE-2015-6111] - Средняя [CVE-2015-6112] - Средняя [CVE-2015-6113] - Низкая [CVE-2015-6125] - Критичная [CVE-2015-6126] - Высокая [CVE-2015-6127] - Средняя [CVE-2015-6128] - Высокая [CVE-2015-6130] - Критичная [CVE-2015-6131] - Критичная [CVE-2015-6132] - Высокая [CVE-2015-6133] - Высокая [CVE-2015-6171] - Высокая [CVE-2015-6173] - Высокая [CVE-2015-6174] - Высокая [CVE-2015-6175] - Высокая [CVE-2016-0006] - Высокая [CVE-2016-0007] - Высокая [CVE-2016-0008] - Средняя [CVE-2016-0009] - Высокая [CVE-2016-0014] - Высокая [CVE-2016-0015] - Высокая [CVE-2016-0016] - Высокая [CVE-2016-0018] - Высокая [CVE-2016-0019] - Высокая [CVE-2016-0020] - Высокая [CVE-2016-0026] - Высокая [CVE-2016-0036] - Высокая [CVE-2016-0037] - Высокая [CVE-2016-0038] - Высокая [CVE-2016-0040] - Высокая [CVE-2016-0041] - Высокая [CVE-2016-0042] - Высокая [CVE-2016-0044] - Высокая [CVE-2016-0046] - Высокая [CVE-2016-0047] - Высокая [CVE-2016-0048] - Высокая [CVE-2016-0049] - Средняя [CVE-2016-0050] - Средняя [CVE-2016-0051] - Высокая [CVE-2016-0058] - Высокая [CVE-2016-0070] - Средняя [CVE-2016-0073] - Средняя [CVE-2016-0075] - Средняя [CVE-2016-0079] - Средняя [CVE-2016-0087] - Высокая [CVE-2016-0088] - Критичная [CVE-2016-0089] - Высокая [CVE-2016-0090] - Высокая [CVE-2016-0091] - Высокая [CVE-2016-0092] - Высокая [CVE-2016-0093] - Высокая [CVE-2016-0094] - Высокая [CVE-2016-0095] - Высокая [CVE-2016-0096] - Высокая [CVE-2016-0098] - Высокая [CVE-2016-0099] - Высокая [CVE-2016-0100] - Высокая [CVE-2016-0101] - Высокая [CVE-2016-0117] - Высокая [CVE-2016-0118] - Высокая [CVE-2016-0120] - Средняя [CVE-2016-0121] - Высокая [CVE-2016-0133] - Средняя [CVE-2016-0135] - Высокая [CVE-2016-0142] - Высокая [CVE-2016-0143] - Высокая [CVE-2016-0145] - Высокая [CVE-2016-0150] - Высокая [CVE-2016-0151] - Высокая [CVE-2016-0152] - Высокая [CVE-2016-0153] - Высокая [CVE-2016-0165] - Высокая [CVE-2016-0167] - Высокая [CVE-2016-0168] - Средняя [CVE-2016-0169] - Средняя [CVE-2016-0170] - Высокая [CVE-2016-0171] - Высокая [CVE-2016-0173] - Высокая [CVE-2016-0174] - Высокая [CVE-2016-0175] - Низкая [CVE-2016-0176] - Высокая [CVE-2016-0179] - Высокая [CVE-2016-0180] - Высокая [CVE-2016-0181] - Средняя [CVE-2016-0182] - Высокая [CVE-2016-0183] - Высокая [CVE-2016-0184] - Высокая [CVE-2016-0185] - Высокая [CVE-2016-0190] - Средняя [CVE-2016-0195] - Высокая [CVE-2016-0196] - Высокая [CVE-2016-0197] - Высокая [CVE-2016-3201] - Средняя [CVE-2016-3203] - Высокая [CVE-2016-3209] - Средняя [CVE-2016-3213] - Высокая [CVE-2016-3215] - Средняя [CVE-2016-3216] - Средняя [CVE-2016-3218] - Высокая [CVE-2016-3219] - Высокая [CVE-2016-3220] - Высокая [CVE-2016-3221] - Высокая [CVE-2016-3223] - Высокая [CVE-2016-3225] - Высокая [CVE-2016-3226] - Средняя [CVE-2016-3227] - Критичная [CVE-2016-3228] - Высокая [CVE-2016-3230] - Средняя [CVE-2016-3232] - Средняя [CVE-2016-3236] - Критичная [CVE-2016-3237] - Высокая [CVE-2016-3238] - Высокая [CVE-2016-3239] - Высокая [CVE-2016-3249] - Высокая [CVE-2016-3250] - Высокая [CVE-2016-3251] - Низкая [CVE-2016-3252] - Высокая [CVE-2016-3254] - Высокая [CVE-2016-3256] - Средняя [CVE-2016-3258] - Средняя [CVE-2016-3262] - Средняя [CVE-2016-3263] - Средняя [CVE-2016-3266] - Высокая [CVE-2016-3270] - Высокая [CVE-2016-3272] - Низкая [CVE-2016-3286] - Высокая [CVE-2016-3287] - Средняя [CVE-2016-3298] - Средняя [CVE-2016-3299] - Средняя [CVE-2016-3300] - Высокая [CVE-2016-3301] - Высокая [CVE-2016-3302] - Средняя [CVE-2016-3303] - Высокая [CVE-2016-3304] - Высокая [CVE-2016-3305] - Высокая [CVE-2016-3306] - Высокая [CVE-2016-3308] - Высокая [CVE-2016-3309] - Высокая [CVE-2016-3310] - Высокая [CVE-2016-3311] - Высокая [CVE-2016-3312] - Критичная [CVE-2016-3319] - Высокая [CVE-2016-3320] - Средняя [CVE-2016-3332] - Высокая [CVE-2016-3333] - Высокая [CVE-2016-3334] - Высокая [CVE-2016-3335] - Высокая [CVE-2016-3338] - Высокая [CVE-2016-3340] - Высокая [CVE-2016-3341] - Высокая [CVE-2016-3342] - Высокая [CVE-2016-3343] - Высокая [CVE-2016-3344] - Низкая [CVE-2016-3345] - Высокая [CVE-2016-3346] - Высокая [CVE-2016-3348] - Высокая [CVE-2016-3349] - Высокая [CVE-2016-3352] - Высокая [CVE-2016-3354] - Низкая [CVE-2016-3355] - Высокая [CVE-2016-3356] - Высокая [CVE-2016-3368] - Высокая [CVE-2016-3369] - Высокая [CVE-2016-3370] - Средняя [CVE-2016-3371] - Средняя [CVE-2016-3372] - Средняя [CVE-2016-3373] - Средняя [CVE-2016-3374] - Средняя [CVE-2016-3375] - Высокая [CVE-2016-3376] - Высокая [CVE-2016-3393] - Высокая [CVE-2016-3396] - Высокая [CVE-2016-5063] - Средняя [CVE-2016-6848] - Средняя [CVE-2016-7165] - Средняя [CVE-2016-7182] - Критичная [CVE-2016-7184] - Высокая [CVE-2016-7185] - Высокая [CVE-2016-7188] - Высокая [CVE-2016-7205] - Высокая [CVE-2016-7210] - Средняя [CVE-2016-7211] - Высокая [CVE-2016-7212] - Высокая [CVE-2016-7214] - Низкая [CVE-2016-7215] - Высокая [CVE-2016-7216] - Средняя [CVE-2016-7217] - Высокая [CVE-2016-7218] - Средняя [CVE-2016-7219] - Средняя [CVE-2016-7220] - Низкая [CVE-2016-7221] - Высокая [CVE-2016-7222] - Высокая [CVE-2016-7223] - Средняя [CVE-2016-7224] - Средняя [CVE-2016-7237] - Средняя [CVE-2016-7238] - Высокая [CVE-2016-7246] - Высокая [CVE-2016-7247] - Высокая [CVE-2016-7248] - Высокая [CVE-2016-7255] - Высокая [CVE-2016-7256] - Высокая [CVE-2016-7257] - Средняя [CVE-2016-7258] - Средняя [CVE-2016-7259] - Высокая [CVE-2016-7260] - Высокая [CVE-2016-7271] - Высокая [CVE-2016-7272] - Высокая [CVE-2016-7273] - Высокая [CVE-2016-7274] - Высокая [CVE-2016-7278] - Средняя [CVE-2016-7292] - Высокая [CVE-2016-7295] - Средняя [CVE-2016-9192] - Высокая [CVE-2016-9459] - Средняя [CVE-2017-0001] - Высокая [CVE-2017-0004] - Высокая [CVE-2017-0005] - Высокая [CVE-2017-0007] - Средняя [CVE-2017-0014] - Высокая [CVE-2017-0016] - Средняя [CVE-2017-0021] - Критичная [CVE-2017-0022] - Средняя [CVE-2017-0024] - Высокая [CVE-2017-0025] - Высокая [CVE-2017-0026] - Высокая [CVE-2017-0038] - Средняя [CVE-2017-0039] - Высокая [CVE-2017-0042] - Низкая [CVE-2017-0043] - Средняя [CVE-2017-0047] - Высокая [CVE-2017-0050] - Высокая [CVE-2017-0051] - Средняя [CVE-2017-0055] - Средняя [CVE-2017-0056] - Высокая [CVE-2017-0057] - Средняя [CVE-2017-0058] - Средняя [CVE-2017-0060] - Средняя [CVE-2017-0061] - Средняя [CVE-2017-0062] - Средняя [CVE-2017-0066] - Средняя [CVE-2017-0072] - Высокая [CVE-2017-0073] - Средняя [CVE-2017-0074] - Средняя [CVE-2017-0075] - Высокая [CVE-2017-0076] - Средняя [CVE-2017-0078] - Высокая [CVE-2017-0080] - Высокая [CVE-2017-0081] - Высокая [CVE-2017-0082] - Высокая [CVE-2017-0083] - Высокая [CVE-2017-0084] - Высокая [CVE-2017-0085] - Средняя [CVE-2017-0086] - Высокая [CVE-2017-0087] - Высокая [CVE-2017-0088] - Высокая [CVE-2017-0089] - Высокая [CVE-2017-0090] - Высокая [CVE-2017-0091] - Средняя [CVE-2017-0092] - Средняя [CVE-2017-0095] - Высокая [CVE-2017-0096] - Низкая [CVE-2017-0097] - Средняя [CVE-2017-0098] - Средняя [CVE-2017-0099] - Средняя [CVE-2017-0100] - Высокая [CVE-2017-0101] - Высокая [CVE-2017-0102] - Высокая [CVE-2017-0103] - Высокая [CVE-2017-0104] - Высокая [CVE-2017-0108] - Высокая [CVE-2017-0109] - Высокая [CVE-2017-0111] - Средняя [CVE-2017-0112] - Средняя [CVE-2017-0113] - Средняя [CVE-2017-0114] - Средняя [CVE-2017-0115] - Средняя [CVE-2017-0116] - Средняя [CVE-2017-0117] - Средняя [CVE-2017-0118] - Средняя [CVE-2017-0119] - Средняя [CVE-2017-0120] - Средняя [CVE-2017-0121] - Средняя [CVE-2017-0122] - Средняя [CVE-2017-0123] - Средняя [CVE-2017-0124] - Средняя [CVE-2017-0125] - Средняя [CVE-2017-0126] - Средняя [CVE-2017-0127] - Средняя [CVE-2017-0128] - Средняя [CVE-2017-0135] - Средняя [CVE-2017-0140] - Средняя [CVE-2017-0143] - Высокая [CVE-2017-0144] - Высокая [CVE-2017-0145] - Высокая [CVE-2017-0146] - Высокая [CVE-2017-0147] - Средняя [CVE-2017-0148] - Высокая [CVE-2017-0154] - Средняя [CVE-2017-0155] - Высокая [CVE-2017-0156] - Высокая [CVE-2017-0158] - Высокая [CVE-2017-0161] - Высокая [CVE-2017-0165] - Высокая [CVE-2017-0171] - Средняя [CVE-2017-0173] - Средняя [CVE-2017-0176] - Высокая [CVE-2017-0178] - Средняя [CVE-2017-0179] - Средняя [CVE-2017-0182] - Средняя [CVE-2017-0183] - Средняя [CVE-2017-0185] - Средняя [CVE-2017-0186] - Средняя [CVE-2017-0190] - Средняя [CVE-2017-0192] - Средняя [CVE-2017-0193] - Высокая [CVE-2017-0199] - Высокая [CVE-2017-0211] - Средняя [CVE-2017-0212] - Высокая [CVE-2017-0213] - Средняя [CVE-2017-0214] - Высокая [CVE-2017-0215] - Средняя [CVE-2017-0216] - Средняя [CVE-2017-0218] - Средняя [CVE-2017-0219] - Средняя [CVE-2017-0250] - Высокая [CVE-2017-0258] - Средняя [CVE-2017-0259] - Средняя [CVE-2017-0263] - Высокая [CVE-2017-0267] - Средняя [CVE-2017-0268] - Средняя [CVE-2017-0269] - Средняя [CVE-2017-0270] - Средняя [CVE-2017-0271] - Средняя [CVE-2017-0272] - Высокая [CVE-2017-0273] - Средняя [CVE-2017-0274] - Средняя [CVE-2017-0275] - Средняя [CVE-2017-0276] - Средняя [CVE-2017-0277] - Высокая [CVE-2017-0278] - Высокая [CVE-2017-0279] - Высокая [CVE-2017-0280] - Средняя [CVE-2017-0282] - Средняя [CVE-2017-0283] - Высокая [CVE-2017-0284] - Средняя [CVE-2017-0285] - Средняя [CVE-2017-0290] - Высокая [CVE-2017-0293] - Высокая [CVE-2017-0294] - Высокая [CVE-2017-0295] - Средняя [CVE-2017-0296] - Высокая [CVE-2017-0297] - Средняя [CVE-2017-0298] - Высокая [CVE-2017-0299] - Средняя [CVE-2017-0300] - Средняя [CVE-2017-10769] - Высокая [CVE-2017-10772] - Высокая [CVE-2017-11762] - Высокая [CVE-2017-11763] - Высокая [CVE-2017-11764] - Высокая [CVE-2017-11765] - Средняя [CVE-2017-11766] - Высокая [CVE-2017-11769] - Высокая [CVE-2017-11771] - Критичная [CVE-2017-11772] - Высокая [CVE-2017-11779] - Высокая [CVE-2017-11780] - Высокая [CVE-2017-11781] - Высокая [CVE-2017-11782] - Высокая [CVE-2017-11783] - Высокая [CVE-2017-11784] - Средняя [CVE-2017-11785] - Средняя [CVE-2017-11790] - Средняя [CVE-2017-11791] - Низкая [CVE-2017-11792] - Высокая [CVE-2017-11793] - Высокая [CVE-2017-11794] - Средняя [CVE-2017-11796] - Высокая [CVE-2017-11798] - Высокая [CVE-2017-11799] - Высокая [CVE-2017-11800] - Высокая [CVE-2017-11802] - Высокая [CVE-2017-11803] - Средняя [CVE-2017-11804] - Высокая [CVE-2017-11805] - Высокая [CVE-2017-11806] - Высокая [CVE-2017-11807] - Высокая [CVE-2017-11808] - Высокая [CVE-2017-11809] - Высокая [CVE-2017-11810] - Высокая [CVE-2017-11811] - Высокая [CVE-2017-11812] - Высокая [CVE-2017-11813] - Высокая [CVE-2017-11814] - Средняя [CVE-2017-11815] - Средняя [CVE-2017-11816] - Средняя [CVE-2017-11817] - Средняя [CVE-2017-11818] - Средняя [CVE-2017-11819] - Высокая [CVE-2017-11821] - Высокая [CVE-2017-11822] - Высокая [CVE-2017-11823] - Средняя [CVE-2017-11824] - Высокая [CVE-2017-11827] - Высокая [CVE-2017-11829] - Средняя [CVE-2017-11832] - Средняя [CVE-2017-11833] - Низкая [CVE-2017-11834] - Средняя [CVE-2017-11835] - Средняя [CVE-2017-11836] - Высокая [CVE-2017-11837] - Высокая [CVE-2017-11838] - Высокая [CVE-2017-11839] - Высокая [CVE-2017-11840] - Высокая [CVE-2017-11841] - Высокая [CVE-2017-11843] - Высокая [CVE-2017-11844] - Средняя [CVE-2017-11845] - Высокая [CVE-2017-11846] - Высокая [CVE-2017-11848] - Средняя [CVE-2017-11850] - Низкая [CVE-2017-11852] - Средняя [CVE-2017-11855] - Высокая [CVE-2017-11856] - Высокая [CVE-2017-11858] - Высокая [CVE-2017-11861] - Высокая [CVE-2017-11862] - Высокая [CVE-2017-11863] - Средняя [CVE-2017-11866] - Высокая [CVE-2017-11869] - Высокая [CVE-2017-11870] - Высокая [CVE-2017-11871] - Высокая [CVE-2017-11872] - Средняя [CVE-2017-11873] - Высокая [CVE-2017-11874] - Низкая [CVE-2017-11886] - Высокая [CVE-2017-11887] - Средняя [CVE-2017-11888] - Высокая [CVE-2017-11889] - Высокая [CVE-2017-11890] - Высокая [CVE-2017-11893] - Высокая [CVE-2017-11894] - Высокая [CVE-2017-11895] - Высокая [CVE-2017-11899] - Критичная [CVE-2017-11901] - Высокая [CVE-2017-11903] - Высокая [CVE-2017-11905] - Высокая [CVE-2017-11906] - Средняя [CVE-2017-11907] - Высокая [CVE-2017-11912] - Высокая [CVE-2017-11913] - Высокая [CVE-2017-11914] - Высокая [CVE-2017-11918] - Высокая [CVE-2017-11919] - Средняя [CVE-2017-11927] - Средняя [CVE-2017-11930] - Высокая [CVE-2017-11937] - Высокая [CVE-2017-11940] - Высокая [CVE-2017-12266] - Средняя [CVE-2017-12312] - Средняя [CVE-2017-12313] - Средняя [CVE-2017-16744] - Высокая [CVE-2017-3222] - Критичная [CVE-2017-3823] - Высокая [CVE-2017-4028] - Средняя [CVE-2017-6638] - Высокая [CVE-2017-6639] - Критичная [CVE-2017-6640] - Критичная [CVE-2017-6753] - Высокая [CVE-2017-7269] - Критичная [CVE-2017-8461] - Высокая [CVE-2017-8462] - Средняя [CVE-2017-8464] - Высокая [CVE-2017-8465] - Высокая [CVE-2017-8467] - Высокая [CVE-2017-8468] - Высокая [CVE-2017-8469] - Средняя [CVE-2017-8470] - Средняя [CVE-2017-8471] - Средняя [CVE-2017-8472] - Средняя [CVE-2017-8473] - Средняя [CVE-2017-8474] - Средняя [CVE-2017-8475] - Средняя [CVE-2017-8476] - Средняя [CVE-2017-8477] - Средняя [CVE-2017-8478] - Средняя [CVE-2017-8479] - Средняя [CVE-2017-8480] - Средняя [CVE-2017-8481] - Средняя [CVE-2017-8482] - Средняя [CVE-2017-8483] - Средняя [CVE-2017-8484] - Средняя [CVE-2017-8485] - Средняя [CVE-2017-8486] - Средняя [CVE-2017-8488] - Средняя [CVE-2017-8489] - Средняя [CVE-2017-8490] - Средняя [CVE-2017-8491] - Средняя [CVE-2017-8492] - Средняя [CVE-2017-8493] - Средняя [CVE-2017-8494] - Высокая [CVE-2017-8495] - Высокая [CVE-2017-8496] - Высокая [CVE-2017-8497] - Высокая [CVE-2017-8498] - Средняя [CVE-2017-8499] - Высокая [CVE-2017-8503] - Высокая [CVE-2017-8504] - Средняя [CVE-2017-8515] - Средняя [CVE-2017-8517] - Высокая [CVE-2017-8519] - Высокая [CVE-2017-8520] - Высокая [CVE-2017-8521] - Высокая [CVE-2017-8522] - Высокая [CVE-2017-8523] - Средняя [CVE-2017-8524] - Высокая [CVE-2017-8528] - Высокая [CVE-2017-8529] - Средняя [CVE-2017-8530] - Средняя [CVE-2017-8531] - Средняя [CVE-2017-8534] - Средняя [CVE-2017-8535] - Средняя [CVE-2017-8536] - Средняя [CVE-2017-8537] - Средняя [CVE-2017-8538] - Высокая [CVE-2017-8539] - Средняя [CVE-2017-8540] - Высокая [CVE-2017-8541] - Высокая [CVE-2017-8542] - Средняя [CVE-2017-8543] - Критичная [CVE-2017-8544] - Средняя [CVE-2017-8547] - Высокая [CVE-2017-8548] - Высокая [CVE-2017-8549] - Высокая [CVE-2017-8552] - Высокая [CVE-2017-8553] - Средняя [CVE-2017-8554] - Средняя [CVE-2017-8555] - Средняя [CVE-2017-8556] - Высокая [CVE-2017-8558] - Высокая [CVE-2017-8561] - Высокая [CVE-2017-8562] - Высокая [CVE-2017-8563] - Высокая [CVE-2017-8564] - Средняя [CVE-2017-8566] - Высокая [CVE-2017-8573] - Высокая [CVE-2017-8574] - Высокая [CVE-2017-8575] - Средняя [CVE-2017-8576] - Высокая [CVE-2017-8577] - Высокая [CVE-2017-8578] - Высокая [CVE-2017-8579] - Высокая [CVE-2017-8580] - Высокая [CVE-2017-8581] - Высокая [CVE-2017-8582] - Средняя [CVE-2017-8588] - Высокая [CVE-2017-8589] - Критичная [CVE-2017-8590] - Высокая [CVE-2017-8592] - Средняя [CVE-2017-8593] - Высокая [CVE-2017-8594] - Высокая [CVE-2017-8595] - Высокая [CVE-2017-8596] - Высокая [CVE-2017-8597] - Средняя [CVE-2017-8598] - Высокая [CVE-2017-8599] - Средняя [CVE-2017-8601] - Высокая [CVE-2017-8602] - Средняя [CVE-2017-8603] - Высокая [CVE-2017-8604] - Высокая [CVE-2017-8605] - Высокая [CVE-2017-8606] - Высокая [CVE-2017-8607] - Высокая [CVE-2017-8608] - Высокая [CVE-2017-8609] - Высокая [CVE-2017-8610] - Высокая [CVE-2017-8611] - Средняя [CVE-2017-8617] - Высокая [CVE-2017-8618] - Высокая [CVE-2017-8619] - Высокая [CVE-2017-8628] - Средняя [CVE-2017-8634] - Высокая [CVE-2017-8635] - Высокая [CVE-2017-8636] - Высокая [CVE-2017-8637] - Средняя [CVE-2017-8638] - Высокая [CVE-2017-8639] - Высокая [CVE-2017-8640] - Высокая [CVE-2017-8641] - Высокая [CVE-2017-8642] - Средняя [CVE-2017-8643] - Средняя [CVE-2017-8644] - Средняя [CVE-2017-8645] - Высокая [CVE-2017-8646] - Высокая [CVE-2017-8647] - Высокая [CVE-2017-8648] - Средняя [CVE-2017-8649] - Высокая [CVE-2017-8650] - Средняя [CVE-2017-8651] - Высокая [CVE-2017-8652] - Средняя [CVE-2017-8653] - Высокая [CVE-2017-8655] - Высокая [CVE-2017-8656] - Высокая [CVE-2017-8657] - Высокая [CVE-2017-8659] - Средняя [CVE-2017-8660] - Высокая [CVE-2017-8661] - Высокая [CVE-2017-8662] - Средняя [CVE-2017-8666] - Средняя [CVE-2017-8668] - Средняя [CVE-2017-8669] - Высокая [CVE-2017-8670] - Высокая [CVE-2017-8671] - Высокая [CVE-2017-8672] - Высокая [CVE-2017-8673] - Средняя [CVE-2017-8674] - Высокая [CVE-2017-8675] - Высокая [CVE-2017-8676] - Низкая [CVE-2017-8677] - Средняя [CVE-2017-8678] - Средняя [CVE-2017-8679] - Средняя [CVE-2017-8680] - Средняя [CVE-2017-8681] - Средняя [CVE-2017-8682] - Высокая [CVE-2017-8683] - Средняя [CVE-2017-8684] - Средняя [CVE-2017-8685] - Средняя [CVE-2017-8687] - Средняя [CVE-2017-8688] - Средняя [CVE-2017-8689] - Высокая [CVE-2017-8692] - Высокая [CVE-2017-8693] - Средняя [CVE-2017-8694] - Высокая [CVE-2017-8695] - Средняя [CVE-2017-8696] - Высокая [CVE-2017-8699] - Высокая [CVE-2017-8702] - Высокая [CVE-2017-8703] - Средняя [CVE-2017-8704] - Средняя [CVE-2017-8706] - Средняя [CVE-2017-8707] - Средняя [CVE-2017-8708] - Средняя [CVE-2017-8709] - Средняя [CVE-2017-8710] - Средняя [CVE-2017-8711] - Средняя [CVE-2017-8712] - Средняя [CVE-2017-8713] - Средняя [CVE-2017-8714] - Высокая [CVE-2017-8715] - Средняя [CVE-2017-8716] - Средняя [CVE-2017-8717] - Высокая [CVE-2017-8718] - Высокая [CVE-2017-8719] - Средняя [CVE-2017-8720] - Высокая [CVE-2017-8723] - Средняя [CVE-2017-8724] - Средняя [CVE-2017-8726] - Средняя [CVE-2017-8727] - Высокая [CVE-2017-8728] - Высокая [CVE-2017-8729] - Высокая [CVE-2017-8731] - Высокая [CVE-2017-8733] - Средняя [CVE-2017-8734] - Высокая [CVE-2017-8735] - Средняя [CVE-2017-8736] - Средняя [CVE-2017-8737] - Высокая [CVE-2017-8738] - Высокая [CVE-2017-8739] - Средняя [CVE-2017-8740] - Высокая [CVE-2017-8741] - Высокая [CVE-2017-8747] - Высокая [CVE-2017-8748] - Высокая [CVE-2017-8749] - Высокая [CVE-2017-8750] - Высокая [CVE-2017-8751] - Высокая [CVE-2017-8752] - Высокая [CVE-2017-8753] - Высокая [CVE-2017-8754] - Средняя [CVE-2017-8755] - Высокая [CVE-2017-8756] - Высокая [CVE-2017-8757] - Высокая [CVE-2017-9511] - Высокая [CVE-2018-0598] - Высокая [CVE-2018-0741] - Средняя [CVE-2018-0749] - Высокая [CVE-2018-0755] - Средняя [CVE-2018-0758] - Высокая [CVE-2018-0760] - Средняя [CVE-2018-0761] - Средняя [CVE-2018-0762] - Высокая [CVE-2018-0763] - Низкая [CVE-2018-0766] - Средняя [CVE-2018-0767] - Средняя [CVE-2018-0768] - Высокая [CVE-2018-0769] - Высокая [CVE-2018-0770] - Высокая [CVE-2018-0771] - Средняя [CVE-2018-0772] - Высокая [CVE-2018-0773] - Высокая [CVE-2018-0774] - Высокая [CVE-2018-0775] - Высокая [CVE-2018-0776] - Высокая [CVE-2018-0777] - Высокая [CVE-2018-0778] - Высокая [CVE-2018-0780] - Средняя [CVE-2018-0781] - Высокая [CVE-2018-0800] - Средняя [CVE-2018-0803] - Средняя [CVE-2018-0811] - Средняя [CVE-2018-0813] - Средняя [CVE-2018-0814] - Средняя [CVE-2018-0815] - Высокая [CVE-2018-0816] - Высокая [CVE-2018-0817] - Высокая [CVE-2018-0824] - Высокая [CVE-2018-0833] - Средняя [CVE-2018-0834] - Высокая [CVE-2018-0835] - Высокая [CVE-2018-0836] - Высокая [CVE-2018-0837] - Высокая [CVE-2018-0838] - Высокая [CVE-2018-0839] - Средняя [CVE-2018-0840] - Высокая [CVE-2018-0847] - Средняя [CVE-2018-0855] - Средняя [CVE-2018-0856] - Высокая [CVE-2018-0857] - Высокая [CVE-2018-0859] - Высокая [CVE-2018-0860] - Высокая [CVE-2018-0861] - Высокая [CVE-2018-0866] - Высокая [CVE-2018-0868] - Высокая [CVE-2018-0872] - Высокая [CVE-2018-0873] - Высокая [CVE-2018-0874] - Высокая [CVE-2018-0876] - Высокая [CVE-2018-0878] - Низкая [CVE-2018-0879] - Высокая [CVE-2018-0881] - Высокая [CVE-2018-0883] - Высокая [CVE-2018-0885] - Средняя [CVE-2018-0886] - Высокая [CVE-2018-0888] - Средняя [CVE-2018-0889] - Высокая [CVE-2018-0891] - Средняя [CVE-2018-0893] - Высокая [CVE-2018-0894] - Средняя [CVE-2018-0895] - Средняя [CVE-2018-0896] - Средняя [CVE-2018-0897] - Средняя [CVE-2018-0898] - Средняя [CVE-2018-0899] - Средняя [CVE-2018-0900] - Средняя [CVE-2018-0901] - Средняя [CVE-2018-0904] - Средняя [CVE-2018-0926] - Средняя [CVE-2018-0927] - Средняя [CVE-2018-0929] - Средняя [CVE-2018-0930] - Высокая [CVE-2018-0931] - Высокая [CVE-2018-0932] - Средняя [CVE-2018-0933] - Высокая [CVE-2018-0934] - Высокая [CVE-2018-0935] - Высокая [CVE-2018-0936] - Высокая [CVE-2018-0937] - Высокая [CVE-2018-0939] - Средняя [CVE-2018-0942] - Низкая [CVE-2018-0952] - Высокая [CVE-2018-0986] - Высокая [CVE-2018-1003] - Высокая [CVE-2018-1009] - Высокая [CVE-2018-1010] - Высокая [CVE-2018-1012] - Высокая [CVE-2018-1013] - Высокая [CVE-2018-1015] - Высокая [CVE-2018-1016] - Высокая [CVE-2018-13399] - Высокая [CVE-2018-15408] - Высокая [CVE-2018-15409] - Высокая [CVE-2018-15410] - Высокая [CVE-2018-15411] - Высокая [CVE-2018-15412] - Высокая [CVE-2018-15413] - Высокая [CVE-2018-15414] - Высокая [CVE-2018-15415] - Высокая [CVE-2018-15416] - Высокая [CVE-2018-15417] - Высокая [CVE-2018-15418] - Высокая [CVE-2018-15419] - Высокая [CVE-2018-15420] - Высокая [CVE-2018-15421] - Высокая [CVE-2018-15422] - Высокая [CVE-2018-15431] - Высокая [CVE-2018-15437] - Средняя [CVE-2018-15490] - Высокая [CVE-2018-16794] - Высокая [CVE-2018-3700] - Средняя [CVE-2018-4858] - Высокая [CVE-2018-5440] - Критичная [CVE-2018-6661] - Высокая [CVE-2018-6664] - Высокая [CVE-2018-6674] - Низкая [CVE-2018-6687] - Средняя [CVE-2018-6690] - Высокая [CVE-2018-6700] - Высокая [CVE-2018-6755] - Высокая [CVE-2018-6756] - Высокая [CVE-2018-6757] - Высокая [CVE-2018-6765] - Высокая [CVE-2018-7249] - Высокая [CVE-2018-7250] - Средняя [CVE-2018-8116] - Средняя [CVE-2018-8218] - Высокая [CVE-2018-8253] - Средняя [CVE-2018-8256] - Высокая [CVE-2018-8307] - Средняя [CVE-2018-8332] - Высокая [CVE-2018-8333] - Высокая [CVE-2018-8335] - Высокая [CVE-2018-8344] - Высокая [CVE-2018-8345] - Высокая [CVE-2018-8346] - Высокая [CVE-2018-8347] - Высокая [CVE-2018-8349] - Высокая [CVE-2018-8350] - Высокая [CVE-2018-8392] - Высокая [CVE-2018-8393] - Высокая [CVE-2018-8407] - Средняя [CVE-2018-8415] - Высокая [CVE-2018-8417] - Средняя [CVE-2018-8420] - Высокая [CVE-2018-8423] - Высокая [CVE-2018-8427] - Средняя [CVE-2018-8432] - Высокая [CVE-2018-8433] - Средняя [CVE-2018-8436] - Средняя [CVE-2018-8437] - Средняя [CVE-2018-8438] - Средняя [CVE-2018-8444] - Средняя [CVE-2018-8471] - Высокая [CVE-2018-8494] - Высокая [CVE-2018-8506] - Средняя [CVE-2018-8547] - Средняя [CVE-2018-8553] - Высокая [CVE-2018-8599] - Высокая [CVE-2018-8634] - Высокая [CVE-2018-8853] - Высокая [CVE-2019-0232] - Высокая [CVE-2019-0543] - Высокая [CVE-2019-0555] - Высокая [CVE-2019-0630] - Высокая [CVE-2019-0633] - Высокая [CVE-2019-0690] - Средняя [CVE-2019-0695] - Средняя [CVE-2019-0701] - Средняя [CVE-2019-0710] - Средняя [CVE-2019-0711] - Средняя [CVE-2019-0712] - Средняя [CVE-2019-0713] - Средняя [CVE-2019-0714] - Средняя [CVE-2019-0715] - Средняя [CVE-2019-0717] - Средняя [CVE-2019-0718] - Средняя [CVE-2019-0723] - Средняя [CVE-2019-0734] - Высокая [CVE-2019-0766] - Высокая [CVE-2019-0885] - Высокая [CVE-2019-0928] - Средняя [CVE-2019-0936] - Высокая [CVE-2019-0966] - Средняя [CVE-2019-1019] - Высокая [CVE-2019-1040] - Средняя [CVE-2019-1074] - Средняя [CVE-2019-1078] - Средняя [CVE-2019-1082] - Высокая [CVE-2019-1089] - Высокая [CVE-2019-1144] - Высокая [CVE-2019-1145] - Высокая [CVE-2019-1148] - Средняя [CVE-2019-1149] - Высокая [CVE-2019-1150] - Высокая [CVE-2019-1151] - Высокая [CVE-2019-1152] - Высокая [CVE-2019-1153] - Средняя [CVE-2019-1166] - Средняя [CVE-2019-1168] - Высокая [CVE-2019-11684] - Критичная [CVE-2019-1172] - Средняя [CVE-2019-1177] - Высокая [CVE-2019-1188] - Высокая [CVE-2019-1198] - Высокая [CVE-2019-1270] - Средняя [CVE-2019-1280] - Высокая [CVE-2019-1309] - Средняя [CVE-2019-1310] - Средняя [CVE-2019-1316] - Высокая [CVE-2019-1317] - Высокая [CVE-2019-1318] - Средняя [CVE-2019-1320] - Высокая [CVE-2019-1321] - Высокая [CVE-2019-1322] - Высокая [CVE-2019-1323] - Высокая [CVE-2019-1336] - Высокая [CVE-2019-1338] - Средняя [CVE-2019-1340] - Высокая [CVE-2019-1381] - Средняя [CVE-2019-1384] - Критичная [CVE-2019-1399] - Средняя [CVE-2019-1409] - Средняя [CVE-2019-1419] - Высокая [CVE-2019-1430] - Высокая [CVE-2019-1456] - Высокая [CVE-2019-1484] - Высокая [CVE-2019-15162] - Средняя [CVE-2019-15283] - Высокая [CVE-2019-15284] - Высокая [CVE-2019-15285] - Высокая [CVE-2019-15286] - Высокая [CVE-2019-15287] - Высокая [CVE-2019-1637] - Высокая [CVE-2019-1638] - Высокая [CVE-2019-1639] - Высокая [CVE-2019-1640] - Высокая [CVE-2019-1641] - Высокая [CVE-2019-1771] - Высокая [CVE-2019-1772] - Высокая [CVE-2019-1773] - Высокая [CVE-2019-18232] - Высокая [CVE-2019-18631] - Высокая [CVE-2019-18913] - Средняя [CVE-2019-1924] - Высокая [CVE-2019-1925] - Высокая [CVE-2019-1926] - Высокая [CVE-2019-1927] - Высокая [CVE-2019-1928] - Высокая [CVE-2019-1929] - Высокая [CVE-2019-19363] - Высокая [CVE-2019-20406] - Высокая [CVE-2019-2390] - Высокая [CVE-2019-3582] - Высокая [CVE-2019-3585] - Высокая [CVE-2019-3587] - Средняя [CVE-2019-3588] - Средняя [CVE-2019-3593] - Высокая [CVE-2019-3610] - Средняя [CVE-2019-3646] - Средняя [CVE-2019-3648] - Средняя [CVE-2019-3654] - Высокая [CVE-2019-3667] - Высокая [CVE-2019-3880] - Средняя [CVE-2019-4732] - Средняя [CVE-2019-6265] - Высокая [CVE-2019-6266] - Критичная [CVE-2019-9510] - Высокая [CVE-2020-0616] - Средняя [CVE-2020-0622] - Средняя [CVE-2020-0635] - Высокая [CVE-2020-0641] - Высокая [CVE-2020-0644] - Высокая [CVE-2020-0661] - Средняя [CVE-2020-0684] - Высокая [CVE-2020-0687] - Высокая [CVE-2020-0729] - Высокая [CVE-2020-0751] - Средняя [CVE-2020-0796] - Критичная [CVE-2020-0799] - Высокая [CVE-2020-0890] - Средняя [CVE-2020-0904] - Средняя [CVE-2020-0921] - Средняя [CVE-2020-0922] - Высокая [CVE-2020-0938] - Высокая [CVE-2020-0965] - Высокая [CVE-2020-0982] - Средняя [CVE-2020-0987] - Средняя [CVE-2020-1005] - Средняя [CVE-2020-1009] - Высокая [CVE-2020-1010] - Высокая [CVE-2020-1013] - Высокая [CVE-2020-1014] - Высокая [CVE-2020-1018] - Высокая [CVE-2020-1020] - Высокая [CVE-2020-1068] - Высокая [CVE-2020-1079] - Высокая [CVE-2020-1083] - Средняя [CVE-2020-1118] - Высокая [CVE-2020-1129] - Высокая [CVE-2020-1160] - Средняя [CVE-2020-1163] - Высокая [CVE-2020-1170] - Высокая [CVE-2020-1206] - Высокая [CVE-2020-1243] - Высокая [CVE-2020-1281] - Высокая [CVE-2020-1284] - Средняя [CVE-2020-1299] - Высокая [CVE-2020-1300] - Высокая [CVE-2020-1301] - Высокая [CVE-2020-13162] - Высокая [CVE-2020-1319] - Высокая [CVE-2020-1351] - Средняя [CVE-2020-1383] - Средняя [CVE-2020-1408] - Высокая [CVE-2020-1421] - Высокая [CVE-2020-1425] - Высокая [CVE-2020-1457] - Высокая [CVE-2020-1471] - Высокая [CVE-2020-1507] - Высокая [CVE-2020-15145] - Высокая [CVE-2020-1560] - Высокая [CVE-2020-1574] - Высокая [CVE-2020-1585] - Высокая [CVE-2020-16877] - Высокая [CVE-2020-16910] - Средняя [CVE-2020-17022] - Высокая [CVE-2020-17162] - Высокая [CVE-2020-24556] - Высокая [CVE-2020-24557] - Высокая [CVE-2020-24562] - Высокая [CVE-2020-25182] - Средняя [CVE-2020-3127] - Высокая [CVE-2020-3128] - Высокая [CVE-2020-3194] - Высокая [CVE-2020-3319] - Низкая [CVE-2020-3321] - Низкая [CVE-2020-3322] - Низкая [CVE-2020-36233] - Высокая [CVE-2020-36603] - Средняя [CVE-2020-4739] - Высокая [CVE-2020-4767] - Высокая [CVE-2020-5384] - Высокая [CVE-2020-7205] - Средняя [CVE-2020-7299] - Средняя [CVE-2020-7320] - Высокая [CVE-2020-7335] - Высокая [CVE-2021-1372] - Средняя [CVE-2021-1710] - Высокая [CVE-2021-21513] - Критичная [CVE-2021-21706] - Средняя [CVE-2021-24076] - Средняя [CVE-2021-24081] - Высокая [CVE-2021-26432] - Критичная [CVE-2021-26433] - Высокая [CVE-2021-26881] - Высокая [CVE-2021-26887] - Высокая [CVE-2021-28317] - Средняя [CVE-2021-31184] - Средняя [CVE-2021-32022] - Средняя [CVE-2021-34439] - Высокая [CVE-2021-34441] - Высокая [CVE-2021-34471] - Высокая [CVE-2021-34503] - Высокая [CVE-2021-34579] - Высокая [CVE-2021-35211] - Критичная [CVE-2021-36745] - Критичная [CVE-2021-36926] - Высокая [CVE-2021-36932] - Высокая [CVE-2021-36933] - Высокая [CVE-2021-38505] - Средняя [CVE-2021-38634] - Высокая [CVE-2021-39032] - Средняя [CVE-2021-40828] - Высокая [CVE-2021-41065] - Высокая [CVE-2021-41330] - Высокая [CVE-2021-42275] - Высокая [CVE-2021-42276] - Высокая [CVE-2022-1794] - Средняя [CVE-2022-21606] - Средняя [CVE-2022-21993] - Высокая [CVE-2022-22516] - Высокая [CVE-2022-22765] - Высокая [CVE-2022-22782] - Высокая [CVE-2022-23235] - Средняя [CVE-2022-23239] - Средняя [CVE-2022-23240] - Средняя [CVE-2022-23609] - Критичная [CVE-2022-23611] - Критичная [CVE-2022-23678] - Средняя [CVE-2022-24765] - Высокая [CVE-2022-24826] - Высокая [CVE-2022-27167] - Высокая [CVE-2022-27608] - Средняя [CVE-2022-27609] - Средняя [CVE-2022-29105] - Высокая [CVE-2022-30190] - Высокая [CVE-2022-32230] - Высокая [CVE-2022-34006] - Высокая [CVE-2022-34478] - Средняя [CVE-2022-34713] - Высокая [CVE-2022-35743] - Высокая [CVE-2022-36670] - Средняя [CVE-2022-37771] - Средняя [CVE-2022-37971] - Высокая [CVE-2022-39327] - Критичная [CVE-2022-40263] - Высокая [CVE-2022-41120] - Высокая [CVE-2022-44704] - Высокая [CVE-2022-45141] - Критичная [CVE-2023-1587] - Средняя [CVE-2023-22880] - Высокая [CVE-2023-28005] - Средняя [CVE-2023-28290] - Средняя [CVE-2023-28297] - Высокая [CVE-2023-31222] - Высокая [CVE-2023-34355] - Высокая [CVE-2023-38175] - Высокая [CVE-2023-38402] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2000-0771] "Microsoft Windows 2000 allows local users to cause a denial of service by corrupting the local security policy via malformed RPC traffic, aka the ""Local Security Policy Corruption"" vulnerability."  
  
[CVE-2001-0509] Vulnerabilities in RPC servers in (1) Microsoft Exchange Server 2000 and earlier, (2) Microsoft SQL Server 2000 and earlier, (3) Windows NT 4.0, and (4) Windows 2000 allow remote attackers to cause a denial of service via malformed inputs.  
  
[CVE-2002-1140] "The Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service (service hang) via malformed packet fragments, aka ""Improper parameter size check leading to denial of service."""  
  
[CVE-2002-1141] "An input validation error in the Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service via malformed fragmented RPC client packets, aka ""Denial of service by sending an invalid RPC request."""  
  
[CVE-2003-0003] Buffer overflow in the RPC Locator service for Microsoft Windows NT 4.0, Windows NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows local users to execute arbitrary code via an RPC call to the service containing certain parameter information.  
  
[CVE-2003-0352] Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms.  
  
[CVE-2003-0807] Buffer overflow in the COM Internet Services and in the RPC over HTTP Proxy components for Microsoft Windows NT Server 4.0, NT 4.0 Terminal Server Edition, 2000, XP, and Server 2003 allows remote attackers to cause a denial of service via a crafted request.  
  
[CVE-2004-0116] An Activation function in the RPCSS Service involved with DCOM activation for Microsoft Windows 2000, XP, and 2003 allows remote attackers to cause a denial of service (memory consumption) via an activation request with a large length field.  
  
[CVE-2004-0124] "The DCOM RPC interface for Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to cause network communications via an ""alter context"" call that contains additional data, aka the ""Object Identity Vulnerability."""  
  
[CVE-2004-0569] The RPC Runtime Library for Microsoft Windows NT 4.0 allows remote attackers to read active memory or cause a denial of service (system crash) via a malicious message, possibly related to improper length values.  
  
[CVE-2005-3644] PNP\_GetDeviceList (upnp\_getdevicelist) in UPnP for Microsoft Windows 2000 SP4 and earlier, and possibly Windows XP SP1 and earlier, allows remote attackers to cause a denial of service (memory consumption) via a DCE RPC request that specifies a large output buffer size, a variant of CVE-2006-6296, and a different vulnerability than CVE-2005-2120.  
  
[CVE-2006-0013] Buffer overflow in the Web Client service (WebClnt.dll) for Microsoft Windows XP SP1 and SP2, and Server 2003 up to SP1, allows remote authenticated users or Guests to execute arbitrary code via crafted RPC requests, a different vulnerability than CVE-2005-1207.  
  
[CVE-2006-0034] Heap-based buffer overflow in the CRpcIoManagerServer::BuildContext function in msdtcprx.dll for Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0 and Windows 2000 SP2 and SP3 allows remote attackers to execute arbitrary code via a long fifth argument to the BuildContextW or BuildContext opcode, which triggers a bug in the NdrAllocate function, aka the MSDTC Invalid Memory Access Vulnerability.  
  
[CVE-2006-2370] "Buffer overflow in the Routing and Remote Access service (RRAS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted ""RPC related requests,"" aka the ""RRAS Memory Corruption Vulnerability."""  
  
[CVE-2006-2371] "Buffer overflow in the Remote Access Connection Manager service (RASMAN) service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted ""RPC related requests,"" that lead to registry corruption and stack corruption, aka the ""RASMAN Registry Corruption Vulnerability."""  
  
[CVE-2006-2380] "Microsoft Windows 2000 SP4 does not properly validate an RPC server during mutual authentication over SSL, which allows remote attackers to spoof an RPC server, aka the ""RPC Mutual Authentication Vulnerability."""  
  
[CVE-2006-3439] Buffer overflow in the Server Service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers, including anonymous users, to execute arbitrary code via a crafted RPC message, a different vulnerability than CVE-2006-1314.  
  
[CVE-2006-4691] Stack-based buffer overflow in the NetpManageIPCConnect function in the Workstation service (wkssvc.dll) in Microsoft Windows 2000 SP4 and XP SP2 allows remote attackers to execute arbitrary code via NetrJoinDomain2 RPC messages with a long hostname.  
  
[CVE-2006-6296] The RpcGetPrinterData function in the Print Spooler (spoolsv.exe) service in Microsoft Windows 2000 SP4 and earlier, and possibly Windows XP SP1 and earlier, allows remote attackers to cause a denial of service (memory consumption) via an RPC request that specifies a large 'offered' value (output buffer size), a variant of CVE-2005-3644.  
  
[CVE-2006-6723] The Workstation service in Microsoft Windows 2000 SP4 and XP SP2 allows remote attackers to cause a denial of service (memory consumption) via a large maxlen value in an NetrWkstaUserEnum RPC request.  
  
[CVE-2007-1748] Stack-based buffer overflow in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 Server SP 4, Server 2003 SP 1, and Server 2003 SP 2 allows remote attackers to execute arbitrary code via a long zone name containing character constants represented by escape sequences.  
  
[CVE-2007-2228] rpcrt4.dll (aka the RPC runtime library) in Microsoft Windows XP SP2, XP Professional x64 Edition, Server 2003 SP1 and SP2, Server 2003 x64 Edition and x64 Edition SP2, and Vista and Vista x64 Edition allows remote attackers to cause a denial of service (RPCSS service stop and system restart) via an RPC request that uses NTLMSSP PACKET authentication with a zero-valued verification trailer signature, which triggers an invalid dereference. NOTE: this also affects Windows 2000 SP4, although the impact is an information leak.  
  
[CVE-2007-3039] Stack-based buffer overflow in the Microsoft Message Queuing (MSMQ) service in Microsoft Windows 2000 Server SP4, Windows 2000 Professional SP4, and Windows XP SP2 allows attackers to execute arbitrary code via a long string in an opnum 0x06 RPC call to port 2103. NOTE: this is remotely exploitable on Windows 2000 Server.  
  
[CVE-2008-3479] "Heap-based buffer overflow in the Microsoft Message Queuing (MSMQ) service (mqsvc.exe) in Microsoft Windows 2000 SP4 allows remote attackers to read memory contents and execute arbitrary code via a crafted RPC call, related to improper processing of parameters to string APIs, aka ""Message Queuing Service Remote Code Execution Vulnerability."""  
  
[CVE-2008-4114] "srv.sys in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via an SMB WRITE\_ANDX packet with an offset that is inconsistent with the packet size, related to ""insufficiently validating the buffer size,"" as demonstrated by a request to the \PIPE\lsarpc named pipe, aka ""SMB Validation Denial of Service Vulnerability."""  
  
[CVE-2008-4250] "The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka ""Server Service Vulnerability."""  
  
[CVE-2009-0079] "The RPCSS service in Microsoft Windows XP SP2 and SP3 and Server 2003 SP1 and SP2 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka ""Windows RPCSS Service Isolation Vulnerability."""  
  
[CVE-2009-0228] "Stack-based buffer overflow in the EnumeratePrintShares function in Windows Print Spooler Service (win32spl.dll) in Microsoft Windows 2000 SP4 allows remote printer servers to execute arbitrary code via a crafted ShareName in a response to an RPC request, related to ""printing data structures,"" aka ""Buffer Overflow in Print Spooler Vulnerability."""  
  
[CVE-2009-0230] "The Windows Print Spooler in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 allows remote authenticated users to gain privileges via a crafted RPC message that triggers loading of a DLL file from an arbitrary directory, aka ""Print Spooler Load Library Vulnerability."""  
  
[CVE-2009-0568] "The RPC Marshalling Engine (aka NDR) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly maintain its internal state, which allows remote attackers to overwrite arbitrary memory locations via a crafted RPC message that triggers incorrect pointer reading, related to ""IDL interfaces containing a non-conformant varying array"" and FC\_SMVARRAY, FC\_LGVARRAY, FC\_VARIABLE\_REPEAT, and FC\_VARIABLE\_OFFSET, aka ""RPC Marshalling Engine Vulnerability."""  
  
[CVE-2009-1544] "Double free vulnerability in the Workstation service in Microsoft Windows allows remote authenticated users to gain privileges via a crafted RPC message to a Windows XP SP2 or SP3 or Server 2003 SP2 system, or cause a denial of service via a crafted RPC message to a Vista Gold, SP1, or SP2 or Server 2008 Gold or SP2 system, aka ""Workstation Service Memory Corruption Vulnerability."""  
  
[CVE-2009-2523] "The License Logging Server (llssrv.exe) in Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via an RPC message containing a string without a null terminator, which triggers a heap-based buffer overflow in the LlsrLicenseRequestW method, aka ""License Logging Server Heap Overflow Vulnerability."""  
  
[CVE-2010-2567] "The RPC client implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly allocate memory during the parsing of responses, which allows remote RPC servers and man-in-the-middle attackers to execute arbitrary code via a malformed response, aka ""RPC Memory Corruption Vulnerability."""  
  
[CVE-2010-2729] "The Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when printer sharing is enabled, does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code, by sending a crafted print request over RPC, as exploited in the wild in September 2010, aka ""Print Spooler Service Impersonation Vulnerability."""  
  
[CVE-2010-2742] "The Netlogon RPC Service in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, and R2, when the domain controller role is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via a crafted RPC packet, aka ""Netlogon RPC Null dereference DOS Vulnerability."""  
  
[CVE-2010-3139] Untrusted search path vulnerability in Microsoft Windows Progman Group Converter (grpconv.exe) allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse imm.dll that is located in the same folder as a .grp file.  
  
[CVE-2010-3222] "Stack-based buffer overflow in the Remote Procedure Call Subsystem (RPCSS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted LPC message that requests an LRPC connection from an LPC server to a client, aka ""LPC Message Buffer Overrun Vulnerability."""  
  
[CVE-2013-3175] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a malformed asynchronous RPC request, aka ""Remote Procedure Call Vulnerability."""  
  
[CVE-2013-3878] "Stack-based buffer overflow in the LRPC client in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges by operating an LRPC server that sends a crafted LPC port message, aka ""LRPC Client Buffer Overrun Vulnerability."""  
  
[CVE-2014-0316] "Memory leak in the Local RPC (LRPC) server implementation in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (memory consumption) and bypass the ASLR protection mechanism via a crafted client that sends messages with an invalid data view, aka ""LRPC ASLR Bypass Vulnerability."""  
  
[CVE-2015-2370] "The authentication implementation in the RPC subsystem in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not prevent DCE/RPC connection reflection, which allows local users to gain privileges via a crafted application, aka ""Windows RPC Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0128] "The SAM and LSAD protocol implementations in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 do not properly establish an RPC channel, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka ""Windows SAM and LSAD Downgrade Vulnerability"" or ""BADLOCK."""  
  
[CVE-2016-0178] "The RPC NDR Engine in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles free operations, which allows remote attackers to execute arbitrary code via malformed RPC requests, aka ""RPC Network Data Representation Engine Elevation of Privilege Vulnerability."""  
  
[CVE-2020-1113] A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.  
  
[CVE-1999-0012] Some web servers under Microsoft Windows allow remote attackers to bypass access restrictions for files with long file names.  
  
[CVE-1999-0227] Access violation in LSASS.EXE (LSA/LSARPC) program in Windows NT allows a denial of service.  
  
[CVE-1999-0228] Denial of service in RPCSS.EXE program (RPC Locator) in Windows NT.  
  
[CVE-1999-0288] The WINS server in Microsoft Windows NT 4.0 before SP4 allows remote attackers to cause a denial of service (process termination) via invalid UDP frames to port 137 (NETBIOS Name Service), as demonstrated via a flood of random packets.  
  
[CVE-1999-0386] Microsoft Personal Web Server and FrontPage Personal Web Server in some Windows systems allows a remote attacker to read files on the server by using a nonstandard URL.  
  
[CVE-1999-0681] Buffer overflow in Microsoft FrontPage Server Extensions (PWS) 3.0.2.926 on Windows 95, and possibly other versions, allows remote attackers to cause a denial of service via a long URL.  
  
[CVE-1999-0749] Buffer overflow in Microsoft Telnet client in Windows 95 and Windows 98 via a malformed Telnet argument.  
  
[CVE-1999-0969] The Windows NT RPC service allows remote attackers to conduct a denial of service using spoofed malformed RPC packets which generate an error message that is sent to the spoofed host, potentially setting up a loop, aka Snork.  
  
[CVE-1999-1127] "Windows NT 4.0 does not properly shut down invalid named pipe RPC connections, which allows remote attackers to cause a denial of service (resource exhaustion) via a series of connections containing malformed data, aka the ""Named Pipes Over RPC"" vulnerability."  
  
[CVE-1999-1291] TCP/IP implementation in Microsoft Windows 95, Windows NT 4.0, and possibly others, allows remote attackers to reset connections by forcing a reset (RST) via a PSH ACK or other means, obtaining the target's last sequence number from the resulting packet, then spoofing a reset to the target.  
  
[CVE-2000-0089] "The rdisk utility in Microsoft Terminal Server Edition and Windows NT 4.0 stores registry hive information in a temporary file with permissions that allow local users to read it, aka the ""RDISK Registry Enumeration File"" vulnerability."  
  
[CVE-2000-0168] "Microsoft Windows 9x operating systems allow an attacker to cause a denial of service via a pathname that includes file device names, aka the ""DOS Device in Path Name"" vulnerability."  
  
[CVE-2000-0216] Microsoft email clients in Outlook, Exchange, and Windows Messaging automatically respond to Read Receipt and Delivery Receipt tags, which could allow an attacker to flood a mail system with responses by forging a Read Receipt request that is redirected to a large distribution list.  
  
[CVE-2000-0228] "Microsoft Windows Media License Manager allows remote attackers to cause a denial of service by sending a malformed request that causes the manager to halt, aka the ""Malformed Media License Request"" Vulnerability."  
  
[CVE-2000-0331] "Buffer overflow in Microsoft command processor (CMD.EXE) for Windows NT and Windows 2000 allows a local user to cause a denial of service via a long environment variable, aka the ""Malformed Environment Variable"" vulnerability."  
  
[CVE-2000-0495] "Microsoft Windows Media Encoder allows remote attackers to cause a denial of service via a malformed request, aka the ""Malformed Windows Media Encoder Request"" vulnerability."  
  
[CVE-2000-0544] Windows NT and Windows 2000 hosts allow a remote attacker to cause a denial of service via malformed DCE/RPC SMBwriteX requests that contain an invalid data length.  
  
[CVE-2000-0653] "Microsoft Outlook Express allows remote attackers to monitor a user's email by creating a persistent browser link to the Outlook Express windows, aka the ""Persistent Mail-Browser Link"" vulnerability."  
  
[CVE-2000-0742] "The IPX protocol implementation in Microsoft Windows 95 and 98 allows remote attackers to cause a denial of service by sending a ping packet with a source IP address that is a broadcast address, aka the ""Malformed IPX Ping Packet"" vulnerability."  
  
[CVE-2000-0790] The web-based folder display capability in Microsoft Internet Explorer 5.5 on Windows 98 allows local users to insert Trojan horse programs by modifying the Folder.htt file and using the InvokeVerb method in the ShellDefView ActiveX control to specify a default execute option for the first file that is listed in the folder.  
  
[CVE-2000-0849] "Race condition in Microsoft Windows Media server allows remote attackers to cause a denial of service in the Windows Media Unicast Service via a malformed request, aka the ""Unicast Service Race Condition"" vulnerability."  
  
[CVE-2000-0858] "Vulnerability in Microsoft Windows NT 4.0 allows remote attackers to cause a denial of service in IIS by sending it a series of malformed requests which cause INETINFO.EXE to fail, aka the ""Invalid URL"" vulnerability."  
  
[CVE-2000-0929] "Microsoft Windows Media Player 7 allows attackers to cause a denial of service in RTF-enabled email clients via an embedded OCX control that is not closed properly, aka the ""OCX Attachment"" vulnerability."  
  
[CVE-2000-0942] "The CiWebHitsFile component in Microsoft Indexing Services for Windows 2000 allows remote attackers to conduct a cross site scripting (CSS) attack via a CiRestriction parameter in a .htw request, aka the ""Indexing Services Cross Site Scripting"" vulnerability."  
  
[CVE-2000-1079] Interactions between the CIFS Browser Protocol and NetBIOS as implemented in Microsoft Windows 95, 98, NT, and 2000 allow remote attackers to modify dynamic NetBIOS name cache entries via a spoofed Browse Frame Request in a unicast or UDP broadcast datagram.  
  
[CVE-2000-1112] "Microsoft Windows Media Player 7 executes scripts in custom skin (.WMS) files, which could allow remote attackers to gain privileges via a skin that contains a malicious script, aka the "".WMS Script Execution"" vulnerability."  
  
[CVE-2000-1113] "Buffer overflow in Microsoft Windows Media Player allows remote attackers to execute arbitrary commands via a malformed Active Stream Redirector (.ASX) file, aka the "".ASX Buffer Overrun"" vulnerability."  
  
[CVE-2000-1217] "Microsoft Windows 2000 before Service Pack 2 (SP2), when running in a non-Windows 2000 domain and using NTLM authentication, and when credentials of an account are locally cached, allows local users to bypass account lockout policies and make an unlimited number of login attempts, aka the ""Domain Account Lockout"" vulnerability."  
  
[CVE-2000-1218] The default configuration for the domain name resolver for Microsoft Windows 98, NT 4.0, 2000, and XP sets the QueryIpMatching parameter to 0, which causes Windows to accept DNS updates from hosts that it did not query, which allows remote attackers to poison the DNS cache.  
  
[CVE-2001-0003] "Web Extender Client (WEC) in Microsoft Office 2000, Windows 2000, and Windows Me does not properly process Internet Explorer security settings for NTLM authentication, which allows attackers to obtain NTLM credentials and possibly obtain the password, aka the ""Web Client NTLM Authentication"" vulnerability."  
  
[CVE-2001-0047] "The default permissions for the MTS Package Administration registry key in Windows NT 4.0 allows local users to install or modify arbitrary Microsoft Transaction Server (MTS) packages and gain privileges, aka one of the ""Registry Permissions"" vulnerabilities."  
  
[CVE-2001-0242] "Buffer overflows in Microsoft Windows Media Player 7 and earlier allow remote attackers to execute arbitrary commands via (1) a long version tag in an .ASX file, or (2) a long banner tag, a variant of the "".ASX Buffer Overrun"" vulnerability as discussed in MS:MS00-090."  
  
[CVE-2001-0245] "Microsoft Index Server 2.0 in Windows NT 4.0, and Indexing Service in Windows 2000, allows remote attackers to read server-side include files via a malformed search request, aka a new variant of the ""Malformed Hit-Highlighting"" vulnerability."  
  
[CVE-2001-0261] Microsoft Windows 2000 Encrypted File System does not properly destroy backups of files that are encrypted, which allows a local attacker to recover the text of encrypted files.  
  
[CVE-2001-0345] Microsoft Windows 2000 telnet service allows attackers to prevent idle Telnet sessions from timing out, causing a denial of service by creating a large number of idle sessions.  
  
[CVE-2001-0346] Handle leak in Microsoft Windows 2000 telnet service allows attackers to cause a denial of service by starting a large number of sessions and terminating them.  
  
[CVE-2001-0347] Information disclosure vulnerability in Microsoft Windows 2000 telnet service allows remote attackers to determine the existence of user accounts such as Guest, or log in to the server without specifying the domain name, via a malformed userid.  
  
[CVE-2001-0348] Microsoft Windows 2000 telnet service allows attackers to cause a denial of service (crash) via a long logon command that contains a backspace.  
  
[CVE-2001-0349] Microsoft Windows 2000 telnet service creates named pipes with predictable names and does not properly verify them, which allows local users to execute arbitrary commands by creating a named pipe with the predictable name and associating a malicious program with it, the first of two variants of this vulnerability.  
  
[CVE-2001-0350] Microsoft Windows 2000 telnet service creates named pipes with predictable names and does not properly verify them, which allows local users to execute arbitrary commands by creating a named pipe with the predictable name and associating a malicious program with it, the second of two variants of this vulnerability.  
  
[CVE-2001-0351] Microsoft Windows 2000 telnet service allows a local user to make a certain system call that allows the user to terminate a Telnet session and cause a denial of service.  
  
[CVE-2001-0504] Vulnerability in authentication process for SMTP service in Microsoft Windows 2000 allows remote attackers to use incorrect credentials to gain privileges and conduct activities such as mail relaying.  
  
[CVE-2001-0541] Buffer overflow in Microsoft Windows Media Player 7.1 and earlier allows remote attackers to execute arbitrary commands via a malformed Windows Media Station (.NSC) file.  
  
[CVE-2001-0662] RPC endpoint mapper in Windows NT 4.0 allows remote attackers to cause a denial of service (loss of RPC services) via a malformed request.  
  
[CVE-2001-0719] Buffer overflow in Microsoft Windows Media Player 6.4 allows remote attackers to execute arbitrary code via a malformed Advanced Streaming Format (ASF) file.  
  
[CVE-2001-0909] Buffer overflow in helpctr.exe program in Microsoft Help Center for Windows XP allows remote attackers to execute arbitrary code via a long hcp: URL.  
  
[CVE-2001-1055] The Microsoft Windows network stack allows remote attackers to cause a denial of service (CPU consumption) via a flood of malformed ARP request packets with random source IP and MAC addresses, as demonstrated by ARPNuke.  
  
[CVE-2001-1200] Microsoft Windows XP allows local users to bypass a locked screen and run certain programs that are associated with Hot Keys.  
  
[CVE-2001-1451] Memory leak in the SNMP LAN Manager (LANMAN) MIB extension for Microsoft Windows 2000 before SP3, when the Print Spooler is not running, allows remote attackers to cause a denial of service (memory consumption) via a large number of GET or GETNEXT requests.  
  
[CVE-2002-0018] In Microsoft Windows NT and Windows 2000, a trusting domain that receives authorization information from a trusted domain does not verify that the trusted domain is authoritative for all listed SIDs, which allows remote attackers to gain Domain Administrator privileges on the trusting domain by injecting SIDs from untrusted domains into the authorization data that comes from from the trusted domain.  
  
[CVE-2002-0034] The Microsoft CONVERT.EXE program, when used on Windows 2000 and Windows XP systems, does not apply the default NTFS permissions when converting a FAT32 file system, which could cause the conversion to produce a file system with less secure permissions than expected.  
  
[CVE-2002-0054] SMTP service in (1) Microsoft Windows 2000 and (2) Internet Mail Connector (IMC) in Exchange Server 5.5 does not properly handle responses to NTLM authentication, which allows remote attackers to perform mail relaying via an SMTP AUTH command using null session credentials.  
  
[CVE-2002-0055] SMTP service in Microsoft Windows 2000, Windows XP Professional, and Exchange 2000 allows remote attackers to cause a denial of service via a command with a malformed data transfer (BDAT) request.  
  
[CVE-2002-0136] Microsoft Internet Explorer 5.5 on Windows 98 allows remote web pages to cause a denial of service (hang) via extremely long values for form fields such as INPUT and TEXTAREA, which can be automatically filled via Javascript.  
  
[CVE-2002-0151] Buffer overflow in Multiple UNC Provider (MUP) in Microsoft Windows operating systems allows local users to cause a denial of service or possibly gain SYSTEM privileges via a long UNC request.  
  
[CVE-2002-0224] The MSDTC (Microsoft Distributed Transaction Service Coordinator) for Microsoft Windows 2000, Microsoft IIS 5.0 and SQL Server 6.5 through SQL 2000 0.0 allows remote attackers to cause a denial of service (crash or hang) via malformed (random) input.  
  
[CVE-2002-0370] Buffer overflow in the ZIP capability for multiple products allows remote attackers to cause a denial of service or execute arbitrary code via ZIP files containing entries with long filenames, including (1) Microsoft Windows 98 with Plus! Pack, (2) Windows XP, (3) Windows ME, (4) Lotus Notes R4 through R6 (pre-gold), (5) Verity KeyView, and (6) Stuffit Expander before 7.0.  
  
[CVE-2002-0372] "Microsoft Windows Media Player versions 6.4 and 7.1 and Media Player for Windows XP allow remote attackers to bypass Internet Explorer's (IE) security mechanisms and run code via an executable .wma media file with a license installation requirement stored in the IE cache, aka the ""Cache Path Disclosure via Windows Media Player""."  
  
[CVE-2002-0373] "The Windows Media Device Manager (WMDM) Service in Microsoft Windows Media Player 7.1 on Windows 2000 systems allows local users to obtain LocalSystem rights via a program that calls the WMDM service to connect to an invalid local storage device, aka ""Privilege Elevation through Windows Media Device Manager Service""."  
  
[CVE-2002-0443] Microsoft Windows 2000 allows local users to bypass the policy that prohibits reusing old passwords by changing the current password before it expires, which does not enable the check for previous passwords.  
  
[CVE-2002-0444] Microsoft Windows 2000 running the Terminal Server 90-day trial version, and possibly other versions, does not apply group policies to incoming users when the number of connections to the SYSVOL share exceeds the maximum, e.g. with a maximum number of licenses, which can allow remote authenticated users to bypass group policies.  
  
[CVE-2002-0597] LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445.  
  
[CVE-2002-0615] "The Windows Media Active Playlist in Microsoft Windows Media Player 7.1 stores information in a well known location on the local file system, allowing attackers to execute HTML scripts in the Local Computer zone, aka ""Media Playback Script Invocation""."  
  
[CVE-2002-0616] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code by attaching an inline macro to an object within an Excel workbook, aka the ""Excel Inline Macros Vulnerability."""  
  
[CVE-2002-0617] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code by creating a hyperlink on a drawing shape in a source workbook that points to a destination workbook containing an autoexecute macro, aka ""Hyperlinked Excel Workbook Macro Bypass."""  
  
[CVE-2002-0618] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code in the Local Computer zone by embedding HTML scripts within an Excel workbook that contains an XSL stylesheet, aka ""Excel XSL Stylesheet Script Execution""."  
  
[CVE-2002-0619] "The Mail Merge Tool in Microsoft Word 2002 for Windows, when Microsoft Access is present on a system, allows remote attackers to execute Visual Basic (VBA) scripts within a mail merge document that is saved in HTML format, aka a ""Variant of MS00-071, Word Mail Merge Vulnerability"" (CVE-2000-0788)."  
  
[CVE-2002-0693] Buffer overflow in the HTML Help ActiveX Control (hhctrl.ocx) in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows remote attackers to execute code via (1) a long parameter to the Alink function, or (2) script containing a long argument to the showHelp function.  
  
[CVE-2002-0694] "The HTML Help facility in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP uses the Local Computer Security Zone when opening .chm files from the Temporary Internet Files folder, which allows remote attackers to execute arbitrary code via HTML mail that references or inserts a malicious .chm file containing shortcuts that can be executed, aka ""Code Execution via Compiled HTML Help File."""  
  
[CVE-2002-0699] Unknown vulnerability in the Certificate Enrollment ActiveX Control in Microsoft Windows 98, Windows 98 Second Edition, Windows Millennium, Windows NT 4.0, Windows 2000, and Windows XP allow remote attackers to delete digital certificates on a user's system via HTML.  
  
[CVE-2002-0724] "Buffer overflow in SMB (Server Message Block) protocol in Microsoft Windows NT, Windows 2000, and Windows XP allows attackers to cause a denial of service (crash) via a SMB\_COM\_TRANSACTION packet with a request for the (1) NetShareEnum, (2) NetServerEnum2, or (3) NetServerEnum3, aka ""Unchecked Buffer in Network Share Provider Can Lead to Denial of Service""."  
  
[CVE-2002-0862] The (1) CertGetCertificateChain, (2) CertVerifyCertificateChainPolicy, and (3) WinVerifyTrust APIs within the CryptoAPI for Microsoft products including Microsoft Windows 98 through XP, Office for Mac, Internet Explorer for Mac, and Outlook Express for Mac, do not properly verify the Basic Constraints of intermediate CA-signed X.509 certificates, which allows remote attackers to spoof the certificates of trusted sites via a man-in-the-middle attack for SSL sessions, as originally reported for Internet Explorer and IIS.  
  
[CVE-2002-0863] "Remote Data Protocol (RDP) version 5.0 in Microsoft Windows 2000 and RDP 5.1 in Windows XP does not encrypt the checksums of plaintext session data, which could allow a remote attacker to determine the contents of encrypted sessions via sniffing, aka ""Weak Encryption in RDP Protocol."""  
  
[CVE-2002-0864] "The Remote Data Protocol (RDP) version 5.1 in Microsoft Windows XP allows remote attackers to cause a denial of service (crash) when Remote Desktop is enabled via a PDU Confirm Active data packet that does not set the Pattern BLT command, aka ""Denial of Service in Remote Desktop."""  
  
[CVE-2002-1139] "The Compressed Folders feature in Microsoft Windows 98 with Plus! Pack, Windows Me, and Windows XP does not properly check the destination folder during the decompression of ZIP files, which allows attackers to place an executable file in a known location on a user's system, aka ""Incorrect Target Path for Zipped File Decompression."""  
  
[CVE-2002-1183] "Microsoft Windows 98 and Windows NT 4.0 do not properly verify the Basic Constraints of digital certificates, allowing remote attackers to execute code, aka ""New Variant of Certificate Validation Flaw Could Enable Identity Spoofing"" (CAN-2002-0862)."  
  
[CVE-2002-1184] The system root folder of Microsoft Windows 2000 has default permissions of Everyone group with Full access (Everyone:F) and is in the search path when locating programs during login or application launch from the desktop, which could allow attackers to gain privileges as other users via Trojan horse programs.  
  
[CVE-2002-1214] Buffer overflow in Microsoft PPTP Service on Windows XP and Windows 2000 allows remote attackers to cause a denial of service (hang) and possibly execute arbitrary code via a certain PPTP packet with malformed control data.  
  
[CVE-2002-1256] The SMB signing capability in the Server Message Block (SMB) protocol in Microsoft Windows 2000 and Windows XP allows attackers to disable the digital signing settings in an SMB session to force the data to be sent unsigned, then inject data into the session without detection, e.g. by modifying group policy information sent from a domain controller.  
  
[CVE-2002-1327] "Buffer overflow in the Windows Shell function in Microsoft Windows XP allows remote attackers to execute arbitrary code via an .MP3 or .WMA audio file with a corrupt custom attribute, aka ""Unchecked Buffer in Windows Shell Could Enable System Compromise."""  
  
[CVE-2002-1561] The RPC component in Windows 2000, Windows NT 4.0, and Windows XP allows remote attackers to cause a denial of service (disabled RPC service) via a malformed packet to the RPC Endpoint Mapper at TCP port 135, which triggers a null pointer dereference.  
  
[CVE-2002-1670] Microsoft Windows XP Professional upgrade edition overwrites previously installed patches for Internet Explorer 6.0, leaving Internet Explorer unpatched.  
  
[CVE-2002-1692] Buffer overflow in backup utility of Microsoft Windows 95 allows attackers to execute arbitrary code by causing a filename with a long extension to be placed in a folder to be backed up.  
  
[CVE-2002-1712] Microsoft Windows 2000 allows remote attackers to cause a denial of service (memory consumption) by sending a flood of empty TCP/IP packets with the ACK and FIN bits set to the NetBIOS port (TCP/139), as demonstrated by stream3.  
  
[CVE-2002-1844] Microsoft Windows Media Player (WMP) 6.3, when installed on Solaris, installs executables with world-writable permissions, which allows local users to delete or modify the executables to gain privileges.  
  
[CVE-2002-1847] Buffer overflow in mplay32.exe of Microsoft Windows Media Player (WMP) 6.3 through 7.1 allows remote attackers to execute arbitrary commands via a long mp3 filename command line argument. NOTE: since the only known attack vector requires command line access, this may not be a vulnerability.  
  
[CVE-2002-1873] Microsoft Exchange 2000, when used with Microsoft Remote Procedure Call (MSRPC), allows remote attackers to cause a denial of service (crash or memory consumption) via malformed MSRPC calls.  
  
[CVE-2002-1932] "Microsoft Windows XP and Windows 2000, when configured to send administrative alerts and the ""Do not overwrite events (clear log manually)"" option is set, does not notify the administrator when the log reaches its maximum size, which allows local users and remote attackers to avoid detection."  
  
[CVE-2002-1933] The terminal services screensaver for Microsoft Windows 2000 does not automatically lock the terminal window if the window is minimized, which could allow local users to gain access to the terminal server window.  
  
[CVE-2002-1984] "Microsoft Internet Explorer 5.0.1 through 6.0 on Windows 2000 or Windows XP allows remote attackers to cause a denial of service (crash) via an OBJECT tag that contains a crafted CLASSID (CLSID) value of ""CLSID:00022613-0000-0000-C000-000000000046""."  
  
[CVE-2002-2073] Cross-site scripting (XSS) vulnerability in the default ASP pages on Microsoft Site Server 3.0 on Windows NT 4.0 allows remote attackers to inject arbitrary web script or HTML via the (1) ctr parameter in Default.asp and (2) the query string to formslogin.asp.  
  
[CVE-2002-2105] Microsoft Windows XP allows local users to prevent the system from booting via a corrupt explorer.exe.manifest file.  
  
[CVE-2002-2117] Microsoft Windows XP allows remote attackers to cause a denial of service (CPU consumption) by flooding UDP port 500 (ISAKMP).  
  
[CVE-2002-2283] "Microsoft Windows XP with Fast User Switching (FUS) enabled does not remove the ""show processes from all users"" privilege when the user is removed from the administrator group, which allows that user to view processes of other users."  
  
[CVE-2003-0004] Buffer overflow in the Windows Redirector function in Microsoft Windows XP allows local users to execute arbitrary code via a long parameter.  
  
[CVE-2003-0009] Cross-site scripting (XSS) vulnerability in Help and Support Center for Microsoft Windows Me allows remote attackers to execute arbitrary script in the Local Computer security context via an hcp:// URL with the malicious script in the topic parameter.  
  
[CVE-2003-0109] Buffer overflow in ntdll.dll on Microsoft Windows NT 4.0, Windows NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows remote attackers to execute arbitrary code, as demonstrated via a WebDAV request to IIS 5.0.  
  
[CVE-2003-0111] "The ByteCode Verifier component of Microsoft Virtual Machine (VM) build 5.0.3809 and earlier, as used in Windows and Internet Explorer, allows remote attackers to bypass security checks and execute arbitrary code via a malicious Java applet, aka ""Flaw in Microsoft VM Could Enable System Compromise."""  
  
[CVE-2003-0227] The logging capability for unicast and multicast transmissions in the ISAPI extension for Microsoft Windows Media Services in Microsoft Windows NT 4.0 and 2000, nsiislog.dll, allows remote attackers to cause a denial of service in Internet Information Server (IIS) and execute arbitrary code via a certain network request.  
  
[CVE-2003-0228] Directory traversal vulnerability in Microsoft Windows Media Player 7.1 and Windows Media Player for Windows XP allows remote attackers to execute arbitrary code via a skins file with a URL containing hex-encoded backslash characters (%5C) that causes an executable to be placed in an arbitrary location.  
  
[CVE-2003-0345] Buffer overflow in the SMB capability for Microsoft Windows XP, 2000, and NT allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is required.  
  
[CVE-2003-0346] Multiple integer overflows in a Microsoft Windows DirectX MIDI library (QUARTZ.DLL) allow remote attackers to execute arbitrary code via a MIDI (.mid) file with (1) large length for a Text or Copyright string, or (2) a large number of tracks, which leads to a heap-based buffer overflow.  
  
[CVE-2003-0348] A certain Microsoft Windows Media Player 9 Series ActiveX control allows remote attackers to view and manipulate the Media Library on the local system via HTML script.  
  
[CVE-2003-0349] Buffer overflow in the streaming media component for logging multicast requests in the ISAPI for the logging capability of Microsoft Windows Media Services (nsiislog.dll), as installed in IIS 5.0, allows remote attackers to execute arbitrary code via a large POST request to nsiislog.dll.  
  
[CVE-2003-0496] Microsoft SQL Server before Windows 2000 SP4 allows local users to gain privileges as the SQL Server user by calling the xp\_fileexist extended stored procedure with a named pipe as an argument instead of a normal file.  
  
[CVE-2003-0533] Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPROMO.LOG log file, as exploited by the Sasser worm.  
  
[CVE-2003-0604] Windows Media Player (WMP) 7 and 8, as running on Internet Explorer and possibly other Microsoft products that process HTML, allows remote attackers to bypass zone restrictions and access or execute arbitrary files via an IFRAME tag pointing to an ASF file whose Content-location contains a File:// URL.  
  
[CVE-2003-0605] The RPC DCOM interface in Windows 2000 SP3 and SP4 allows remote attackers to cause a denial of service (crash), and local attackers to use the DoS to hijack the epmapper pipe to gain privileges, via certain messages to the \_\_RemoteGetClassObject interface that cause a NULL pointer to be passed to the PerformScmStage function.  
  
[CVE-2003-0660] The Authenticode capability in Microsoft Windows NT through Server 2003 does not prompt the user to download and install ActiveX controls when the system is low on memory, which could allow remote attackers to execute arbitrary code without user approval.  
  
[CVE-2003-0662] Buffer overflow in Troubleshooter ActiveX Control (Tshoot.ocx) in Microsoft Windows 2000 SP4 and earlier allows remote attackers to execute arbitrary code via an HTML document with a long argument to the RunQuery2 method.  
  
[CVE-2003-0719] Buffer overflow in the Private Communications Transport (PCT) protocol implementation in the Microsoft SSL library, as used in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via PCT 1.0 handshake packets.  
  
[CVE-2003-0806] Buffer overflow in the Windows logon process (winlogon) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, and XP SP1, when a member of a domain, allows remote attackers to execute arbitrary code.  
  
[CVE-2003-0812] "Stack-based buffer overflow in a logging function for Windows Workstation Service (WKSSVC.DLL) allows remote attackers to execute arbitrary code via RPC calls that cause long entries to be written to a debug log file (""NetSetup.LOG""), as demonstrated using the NetAddAlternateComputerName API."  
  
[CVE-2003-0813] A multi-threaded race condition in the Windows RPC DCOM functionality with the MS03-039 patch installed allows remote attackers to cause a denial of service (crash or reboot) by causing two threads to process the same RPC request, which causes one thread to use memory after it has been freed, a different vulnerability than CVE-2003-0352 (Blaster/Nachi), CVE-2003-0715, and CVE-2003-0528, and as demonstrated by certain exploits against those vulnerabilities.  
  
[CVE-2003-0818] Multiple integer overflows in Microsoft ASN.1 library (MSASN1.DLL), as used in LSASS.EXE, CRYPT32.DLL, and other Microsoft executables and libraries on Windows NT 4.0, 2000, and XP, allow remote attackers to execute arbitrary code via ASN.1 BER encodings with (1) very large length fields that cause arbitrary heap data to be overwritten, or (2) modified bit strings.  
  
[CVE-2003-0825] The Windows Internet Naming Service (WINS) for Microsoft Windows Server 2003, and possibly Windows NT and Server 2000, does not properly validate the length of certain packets, which allows attackers to cause a denial of service and possibly execute arbitrary code.  
  
[CVE-2003-0839] "Directory traversal vulnerability in the ""Shell Folders"" capability in Microsoft Windows Server 2003 allows remote attackers to read arbitrary files via .. (dot dot) sequences in a ""shell:"" link."  
  
[CVE-2003-0906] Buffer overflow in the rendering for (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, and XP SP1 allows remote attackers to execute arbitrary code via a malformed WMF or EMF image.  
  
[CVE-2003-0907] Help and Support Center in Microsoft Windows XP SP1 does not properly validate HCP URLs, which allows remote attackers to execute arbitrary code via quotation marks in an hcp:// URL, which are not quoted when constructing the argument list to HelpCtr.exe.  
  
[CVE-2003-0908] "The Utility Manager in Microsoft Windows 2000 executes winhlp32.exe with system privileges, which allows local users to execute arbitrary code via a ""Shatter"" style attack using a Windows message that accesses the context sensitive help button in the GUI, as demonstrated using the File Open dialog in the Help window, a different vulnerability than CVE-2004-0213."  
  
[CVE-2003-0995] Buffer overflow in the Microsoft Message Queue Manager (MSQM) allows remote attackers to cause a denial of service (RPC service crash) via a queue registration request.  
  
[CVE-2003-1106] The SMTP service in Microsoft Windows 2000 before SP4 allows remote attackers to cause a denial of service (crash or hang) via an e-mail message with a malformed time stamp in the FILETIME attribute.  
  
[CVE-2003-1107] The DHTML capability in Microsoft Windows Media Player (WMP) 6.4, 7.0, 7.1, and 9 may run certain URL commands from a security zone that is less trusted than the current zone, which allows attackers to bypass intended access restrictions.  
  
[CVE-2004-0120] The Microsoft Secure Sockets Layer (SSL) library, as used in Windows 2000, Windows XP, and Windows Server 2003, allows remote attackers to cause a denial of service via malformed SSL messages.  
  
[CVE-2004-0199] Help and Support Center in Microsoft Windows XP and Windows Server 2003 SP1 does not properly validate HCP URLs, which allows remote attackers to execute arbitrary code, as demonstrated using certain hcp:// URLs that access the DVD Upgrade capability (dvdupgrd.htm).  
  
[CVE-2004-0201] Heap-based buffer overflow in the HtmlHelp program (hh.exe) in HTML Help for Microsoft Windows 98, Me, NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary commands via a .CHM file with a large length field, a different vulnerability than CVE-2003-1041.  
  
[CVE-2004-0202] IDirectPlay4 Application Programming Interface (API) of Microsoft DirectPlay 7.0a thru 9.0b, as used in Windows Server 2003 and earlier allows remote attackers to cause a denial of service (application crash) via a malformed packet.  
  
[CVE-2004-0206] "Network Dynamic Data Exchange (NetDDE) services for Microsoft Windows 98, Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows attackers to remotely execute arbitrary code or locally gain privileges via a malicious message or application that involves an ""unchecked buffer,"" possibly a buffer overflow."  
  
[CVE-2004-0207] """Shatter"" style vulnerability in the Window Management application programming interface (API) for Microsoft Windows 98, Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows local users to gain privileges by using certain API functions to change properties of privileged programs using the SetWindowLong and SetWIndowLongPtr API functions."  
  
[CVE-2004-0208] The Virtual DOS Machine (VDM) subsystem of Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows local users to access kernel memory and gain privileges via a malicious program that modified some system structures in a way that is not properly validated by privileged operating system functions.  
  
[CVE-2004-0209] "Unknown vulnerability in the Graphics Rendering Engine processes of Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code via (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats that involve ""an unchecked buffer."""  
  
[CVE-2004-0210] The POSIX component of Microsoft Windows NT and Windows 2000 allows local users to execute arbitrary code via certain parameters, possibly by modifying message length values and causing a buffer overflow.  
  
[CVE-2004-0211] The kernel for Microsoft Windows Server 2003 does not reset certain values in CPU data structures, which allows local users to cause a denial of service (system crash) via a malicious program.  
  
[CVE-2004-0214] Buffer overflow in Microsoft Internet Explorer and Explorer on Windows XP SP1, WIndows 2000, Windows 98, and Windows Me may allow remote malicious servers to cause a denial of service (application crash) and possibly execute arbitrary code via long share names, as demonstrated using Samba.  
  
[CVE-2004-0503] Microsoft Outlook 2003 allows remote attackers to bypass the default zone restrictions and execute script within media files via a Rich Text Format (RTF) message containing an OLE object for the Windows Media Player, which bypasses Media Player's setting to disallow scripting and may lead to unprompted installation of an executable when exploited in conjunction with predictable-file-location exposures such as CVE-2004-0502.  
  
[CVE-2004-0540] Microsoft Windows 2000, when running in a domain whose Fully Qualified Domain Name (FQDN) is exactly 8 characters long, does not prevent users with expired passwords from logging on to the domain.  
  
[CVE-2004-0571] "Microsoft Word for Windows 6.0 Converter does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka ""Table Conversion Vulnerability,"" a different vulnerability than CVE-2004-0901."  
  
[CVE-2004-0572] Buffer overflow in the Windows Program Group Converter (grpconv.exe) may allow remote attackers to execute arbitrary code via a shell: URL with a long filename and a .grp extension, which is not properly handled when the shell capability launches grpconv.exe.  
  
[CVE-2004-0574] "The Network News Transfer Protocol (NNTP) component of Microsoft Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003, Exchange 2000 Server, and Exchange Server 2003 allows remote attackers to execute arbitrary code via XPAT patterns, possibly related to improper length validation and an ""unchecked buffer,"" leading to off-by-one and heap-based buffer overflows."  
  
[CVE-2004-0575] "Integer overflow in DUNZIP32.DLL for Microsoft Windows XP, Windows XP 64-bit Edition, Windows Server 2003, and Windows Server 2003 64-bit Edition allows remote attackers to execute arbitrary code via compressed (zipped) folders that involve an ""unchecked buffer"" and improper length validation."  
  
[CVE-2004-0726] The Windows Media Player control in Microsoft Windows 2000 allows remote attackers to execute arbitrary script in the local computer zone via an ASX filename that contains javascript, which is executed in the local context in a preview panel.  
  
[CVE-2004-0727] "Microsoft Internet Explorer 6.0.2800.1106 on Microsoft Windows XP SP2, and other versions including 5.01 and 5.5, allows remote web servers to bypass zone restrictions and execute arbitrary code in the local computer zone by redirecting a function to another function with the same name, as demonstrated by SimilarMethodNameRedir, aka the ""Similar Method Name Redirection Cross Domain Vulnerability."""  
  
[CVE-2004-0840] The SMTP (Simple Mail Transfer Protocol) component of Microsoft Windows XP 64-bit Edition, Windows Server 2003, Windows Server 2003 64-bit Edition, and the Exchange Routing Engine component of Exchange Server 2003, allows remote attackers to execute arbitrary code via a malicious DNS response message containing length values that are not properly validated.  
  
[CVE-2004-0897] The Indexing Service for Microsoft Windows XP and Server 2003 does not properly validate the length of a message, which allows remote attackers to execute arbitrary code via a buffer overflow attack.  
  
[CVE-2004-0899] "The DHCP Server service for Microsoft Windows NT 4.0 Server and Terminal Server Edition, with DHCP logging enabled, does not properly validate the length of certain messages, which allows remote attackers to cause a denial of service (application crash) via a malformed DHCP message, aka ""Logging Vulnerability."""  
  
[CVE-2004-0900] "The DHCP Server service for Microsoft Windows NT 4.0 Server and Terminal Server Edition does not properly validate the length of certain messages, which allows remote attackers to execute arbitrary code via a malformed DHCP message, aka the ""DHCP Request Vulnerability."""  
  
[CVE-2004-0901] "Microsoft Word for Windows 6.0 Converter (MSWRD632.WPC), as used in WordPad, does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka ""Font Conversion Vulnerability,"" a different vulnerability than CVE-2004-0571."  
  
[CVE-2004-1049] "Integer overflow in the LoadImage API of the USER32 Lib for Microsoft Windows allows remote attackers to execute arbitrary code via a .bmp, .cur, .ico or .ani file with a large image size field, which leads to a buffer overflow, aka the ""Cursor and Icon Format Handling Vulnerability."""  
  
[CVE-2004-1080] "The WINS service (wins.exe) on Microsoft Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 allows remote attackers to write to arbitrary memory locations and possibly execute arbitrary code via a modified memory pointer in a WINS replication packet to TCP port 42, aka the ""Association Context Vulnerability."""  
  
[CVE-2004-1324] The Microsoft Windows Media Player 9.0 ActiveX control may allow remote attackers to execute arbitrary web script in the Local computer zone via the (1) artist or (2) song fields of a music file, if the file is processed using Internet Explorer.  
  
[CVE-2004-1325] The getItemInfoByAtom function in the ActiveX control for Microsoft Windows Media Player 9.0 returns a 0 if the file does not exist and the size of the file if the file exists, which allows remote attackers to determine the existence of files on the local system.  
  
[CVE-2004-1889] Unknown vulnerability in ftpd in SGI IRIX 6.5.20 through 6.5.23 allows remote attackers to cause a denial of service (hang) via a link failure with Microsoft Windows.  
  
[CVE-2004-2176] The Internet Connection Firewall (ICF) in Microsoft Windows XP SP2 is configured by default to trust sessmgr.exe, which allows local users to use sessmgr.exe to create a local listening port that bypasses the ICF access controls.  
  
[CVE-2004-2289] Microsoft Windows XP Explorer allows local users to execute arbitrary code via a system folder with a Desktop.ini file containing a .ShellClassInfo specifier with a CLSID value that is associated with an executable file.  
  
[CVE-2004-2290] Microsoft Windows XP Explorer allows attackers to execute arbitrary code via a HTML and script in a self-executing folder that references an executable file within the folder, which is automatically executed when a user accesses the folder.  
  
[CVE-2004-2291] Microsoft Windows Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via an embedded script that uses Shell Helper objects and a shortcut (link) to execute the target script.  
  
[CVE-2004-2307] Microsoft Internet Explorer 6.0.2600 on Windows XP allows remote attackers to cause a denial of service (browser crash) via a shell: URI with double backslashes (\\) in an HTML tag such as IFRAME or A.  
  
[CVE-2004-2339] \*\* DISPUTED \*\* Microsoft Windows 2000, XP, and possibly 2003 allows local users with the SeDebugPrivilege privilege to execute arbitrary code as kernel and read or write kernel memory via the NtSystemDebugControl function, which does not verify its pointer arguments. Note: this issue has been disputed, since Administrator privileges are typically required to exploit this issue, thus privilege boundaries are not crossed.  
  
[CVE-2004-2365] Memory leak in Microsoft Windows XP and Windows Server 2003 allows local users to cause a denial of service (memory exhaustion) by repeatedly creating and deleting directories using a non-standard tool such as smbmount.  
  
[CVE-2004-2454] aMSN 0.90 for Microsoft Windows allows local users to obtain sensitive information such as hashed passwords from (1) hotlog.htm and (2) config.xml.  
  
[CVE-2004-2527] "The local and remote desktop login screens in Microsoft Windows XP before SP2 and 2003 allow remote attackers to cause a denial of service (CPU and memory consumption) by repeatedly using the WinKey+""U"" key combination, which causes multiple copies of Windows Utility Manager to be loaded more quickly than they can be closed when the copies detect that another instance is running."  
  
[CVE-2005-0048] "Microsoft Windows XP SP2 and earlier, 2000 SP3 and SP4, Server 2003, and older operating systems allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted IP packets with malformed options, aka the ""IP Validation Vulnerability."""  
  
[CVE-2005-0058] Buffer overflow in the Telephony Application Programming Interface (TAPI) for Microsoft Windows 98, Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Server 2003 allows attackers to elevate privileges or execute arbitrary code via a crafted message.  
  
[CVE-2005-0059] Buffer overflow in the Message Queuing component of Microsoft Windows 2000 and Windows XP SP1 allows remote attackers to execute arbitrary code via a crafted message.  
  
[CVE-2005-0060] Buffer overflow in the font processing component of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via a specially-designed application.  
  
[CVE-2005-0061] The kernel of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via certain access requests.  
  
[CVE-2005-0063] The document processing application used by the Windows Shell in Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code by modifying the CLSID stored in a file so that it is processed by HTML Application Host (MSHTA), as demonstrated using a Microsoft Word document.  
  
[CVE-2005-0545] Microsoft Windows XP Pro SP2 and Windows 2000 Server SP4 running Active Directory allow local users to bypass group policies that restrict access to hidden drives by using the browse feature in Office 10 applications such as Word or Excel, or using a flash drive. NOTE: this issue has been disputed in a followup post.  
  
[CVE-2005-0550] "Buffer overflow in Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to cause a denial of service (i.e., system crash) via a malformed request, aka ""Object Management Vulnerability""."  
  
[CVE-2005-0551] Stack-based buffer overflow in WINSRV.DLL in the Client Server Runtime System (CSRSS) process of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via a specially-designed application that provides console window information with a long FaceName value.  
  
[CVE-2005-0771] VERITAS Backup Exec Server (beserver.exe) 9.0 through 10.0 for Windows allows remote unauthenticated attackers to modify the registry by calling methods to the RPC interface on TCP port 6106.  
  
[CVE-2005-0852] Microsoft Windows XP SP1 allows local users to cause a denial of service (system crash) via an empty datagram to a raw IP over IP socket (IP protocol 4), as originally demonstrated using code in Python 2.3.  
  
[CVE-2005-1205] The Telnet client for Microsoft Windows XP, Windows Server 2003, and Windows Services for UNIX allows remote attackers to read sensitive environment variables via the NEW-ENVIRON option with a SEND ENV\_USERVAR command.  
  
[CVE-2005-1206] "Buffer overflow in the Server Message Block (SMB) functionality for Microsoft Windows 2000, XP SP1 and SP2, and Server 2003 and SP1 allows remote attackers to execute arbitrary code via unknown vectors, aka the ""Server Message Block Vulnerability."""  
  
[CVE-2005-1207] Buffer overflow in the Web Client service in Microsoft Windows XP and Windows Server 2003 allows remote authenticated users to execute arbitrary code via a crafted WebDAV request containing special parameters.  
  
[CVE-2005-1208] "Integer overflow in Microsoft Windows 98, 2000, XP SP2 and earlier, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via a crafted compiled Help (.CHM) file with a large size field that triggers a heap-based buffer overflow, as demonstrated using a ""ms-its:"" URL in Internet Explorer."  
  
[CVE-2005-1218] The Microsoft Windows kernel in Microsoft Windows 2000 Server, Windows XP, and Windows Server 2003 allows remote attackers to cause a denial of service (crash) via crafted Remote Desktop Protocol (RDP) requests.  
  
[CVE-2005-1219] Buffer overflow in the Microsoft Color Management Module for Windows allows remote attackers to execute arbitrary code via an image with crafted ICC profile format tags.  
  
[CVE-2005-1792] Memory leak in Windows Management Instrumentation (WMI) service allows attackers to cause a denial of service (memory consumption and crash) by creating security contexts more quickly than they can be cleared from the RPC cache.  
  
[CVE-2005-1793] User32.DLL in Microsoft Windows 98SE, and possibly other operating systems, allows local and remote attackers to cause a denial of service (crash) via an icon (.ico) bitmap file with large width and height values.  
  
[CVE-2005-1978] "COM+ in Microsoft Windows does not properly ""create and use memory structures,"" which allows local users or remote attackers to execute arbitrary code."  
  
[CVE-2005-1979] "Distributed Transaction Controller in Microsoft Windows allows remote servers to cause a denial of service (MSDTC service exception and exit) via an ""unexpected protocol command during the reconnection request,"" which is not properly handled by the Transaction Internet Protocol (TIP) functionality."  
  
[CVE-2005-1980] "Distributed Transaction Controller in Microsoft Windows allows remote servers to cause a denial of service (MSDTC service hang) via a crafted Transaction Internet Protocol (TIP) message that causes DTC to repeatedly connect to a target IP and port number after an error occurs, aka the ""Distributed TIP Vulnerability."""  
  
[CVE-2005-1981] Unknown vulnerability in Microsoft Windows 2000 Server and Windows Server 2003 domain controllers allows remote authenticated users to cause a denial of service (system crash) via a crafted Kerberos message.  
  
[CVE-2005-1982] Unknown vulnerability in the PKINIT Protocol for Microsoft Windows 2000, Windows XP, and Windows Server 2003 could allow a local user to obtain information and spoof a server via a man-in-the-middle (MITM) attack between a client and a domain controller when PKINIT smart card authentication is being used.  
  
[CVE-2005-1983] Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm.  
  
[CVE-2005-1984] Buffer overflow in the Print Spooler service (Spoolsv.exe) for Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code via a malicious message.  
  
[CVE-2005-1985] "The Client Service for NetWare (CSNW) on Microsoft Windows 2000 SP4, XP SP1 and Sp2, and Server 2003 SP1 and earlier, allows remote attackers to execute arbitrary code due to an ""unchecked buffer"" when processing certain crafted network messages."  
  
[CVE-2005-1987] "Buffer overflow in Collaboration Data Objects (CDO), as used in Microsoft Windows and Microsoft Exchange Server, allows remote attackers to execute arbitrary code when CDOSYS or CDOEX processes an e-mail message with a large header name, as demonstrated using the ""Content-Type"" string."  
  
[CVE-2005-2117] Web View in Windows Explorer on Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 does not properly handle certain HTML characters in preview fields, which allows remote user-assisted attackers to execute arbitrary code.  
  
[CVE-2005-2118] Windows Shell for Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote user-assisted attackers to execute arbitrary commands via a crafted shortcut (.lnk) file with long font properties that lead to a buffer overflow when the user views the file's properties using Windows Explorer, a different vulnerability than CVE-2005-2122.  
  
[CVE-2005-2120] "Stack-based buffer overflow in the Plug and Play (PnP) service (UMPNPMGR.DLL) in Microsoft Windows 2000 SP4, and XP SP1 and SP2, allows remote or local authenticated attackers to execute arbitrary code via a large number of ""\"" (backslash) characters in a registry key name, which triggers the overflow in a wsprintfW function call."  
  
[CVE-2005-2122] Windows Shell for Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to execute arbitrary commands via a shortcut (.lnk) file with long font properties that lead to a buffer overflow in the Client/Server Runtime Server Subsystem (CSRSS), a different vulnerability than CVE-2005-2118.  
  
[CVE-2005-2128] QUARTZ.DLL in Microsoft Windows Media Player 9 allows remote attackers to write a null byte to arbitrary memory via an AVI file with a crafted strn element with a modified length value.  
  
[CVE-2005-2224] aspnet\_wp.exe in Microsoft ASP.NET web services allows remote attackers to cause a denial of service (CPU consumption from infinite loop) via a crafted SOAP message to an RPC/Encoded method.  
  
[CVE-2005-2307] "netman.dll in Microsoft Windows Connections Manager Library allows local users to cause a denial of service (Network Connections Service crash) via a large integer argument to a particular function, aka ""Network Connection Manager Vulnerability."""  
  
[CVE-2005-2388] Buffer overflow in a certain USB driver, as used on Microsoft Windows, allows attackers to execute arbitrary code.  
  
[CVE-2005-2935] Unquoted Windows search path vulnerability in Microsoft AntiSpyware might allow local users to execute code via a malicious c:\program.exe file, which is run by AntiSpywareMain.exe when it attempts to execute gsasDtServ.exe. NOTE: it is not clear whether this overlaps CVE-2005-2940.  
  
[CVE-2005-2940] "Unquoted Windows search path vulnerability in Microsoft Antispyware 1.0.509 (Beta 1) might allow local users to gain privileges via a malicious ""program.exe"" file in the C: folder, involving the programs (1) GIANTAntiSpywareMain.exe, (2) gcASNotice.exe, (3) gcasServ.exe, (4) gcasSWUpdater.exe, or (5) GIANTAntiSpywareUpdater.exe. NOTE: it is not clear whether this overlaps CVE-2005-2935."  
  
[CVE-2005-3168] The SECEDIT command on Microsoft Windows 2000 before Update Rollup 1 for SP4, when using a security template to set Access Control Lists (ACLs) on folders, does not apply ACLs on folders that are listed after a long folder entry, which could result in less secure permissions than specified by the template.  
  
[CVE-2005-3169] "Microsoft Windows 2000 before Update Rollup 1 for SP4, when the ""audit directory service access"" policy is enabled, does not record a 565 event message for File Delete Child operations on an Active Directory object in the security event log, which could allow attackers to conduct unauthorized activities without detection."  
  
[CVE-2005-3170] The LDAP client on Microsoft Windows 2000 before Update Rollup 1 for SP4 accepts certificates using LDAP Secure Sockets Layer (LDAPS) even when the Certificate Authority (CA) is not trusted, which could allow attackers to trick users into believing that they are accessing a trusted site.  
  
[CVE-2005-3171] Microsoft Windows 2000 before Update Rollup 1 for SP4 records Event ID 1704 to indicate that Group Policy security settings were successfully updated, even when the processing fails such as when Ntuser.pol cannot be accessed, which could cause system administrators to believe that the system is compliant with the specified settings.  
  
[CVE-2005-3172] The WideCharToMultiByte function in Microsoft Windows 2000 before Update Rollup 1 for SP4 does not properly convert strings with Japanese composite characters in the last character, which could prevent the string from being null terminated and lead to data corruption or enable buffer overflow attacks.  
  
[CVE-2005-3173] Microsoft Windows 2000 before Update Rollup 1 for SP4 does not apply group policies if the user logs on using UPN credentials with a trailing dot, which prevents Windows 2000 from finding the correct domain controller and could allow the user to bypass intended restrictions.  
  
[CVE-2005-3174] Microsoft Windows 2000 before Update Rollup 1 for SP4 allows users to log on to the domain, even when their password has expired, if the fully qualified domain name (FQDN) is 8 characters long.  
  
[CVE-2005-3175] Microsoft Windows 2000 before Update Rollup 1 for SP4 allows a local administrator to unlock a computer even if it has been locked by a domain administrator, which allows the local administrator to access the session as the domain administrator.  
  
[CVE-2005-3176] Microsoft Windows 2000 before Update Rollup 1 for SP4 does not record the IP address of a Windows Terminal Services client in a security log event if the client connects successfully, which could make it easier for attackers to escape detection.  
  
[CVE-2005-3177] CHKDSK in Microsoft Windows 2000 before Update Rollup 1 for SP4, Windows XP, and Windows Server 2003, when running in fix mode, does not properly handle security descriptors if the master file table contains a large number of files or if the descriptors do not satisfy certain NTFS conventions, which could cause ACLs for some files to be reverted to less secure defaults, or cause security descriptors to be removed.  
  
[CVE-2005-3595] By default Microsoft Windows XP Home Edition installs with a blank password for the Administrator account, which allows remote attackers to gain control of the computer.  
  
[CVE-2005-3945] The SynAttackProtect protection in Microsoft Windows 2003 before SP1 and Windows 2000 before SP4 with Update Roll-up uses a hash of predictable data, which allows remote attackers to cause a denial of service (CPU consumption) via a flood of SYN packets that produce identical hash values, which slows down the hash table lookups.  
  
[CVE-2005-3981] \*\* DISPUTED \*\* NOTE: this issue has been disputed by third parties. Microsoft Windows XP, 2000, and 2003 allows local users to kill a writable process by using the CreateRemoteThread function with certain arguments on a process that has been opened using the OpenProcess function, possibly involving an invalid address for the start routine. NOTE: followup posts have disputed this issue, saying that if a user already has privileges to write to a process, then other functions could be called or the process could be terminated using PROCESS\_TERMINATE.  
  
[CVE-2005-4269] "mshtml.dll in Microsoft Windows XP, Server 2003, and Internet Explorer 6.0 SP1 allows attackers to cause a denial of service (access violation) by causing mshtml.dll to process button-focus events at the same time that a document is reloading, as seen in Microsoft Office InfoPath 2003 by repeatedly clicking the ""Delete"" button in a repeating section in a form. NOTE: the normal operation of InfoPath appears to involve a local user without any privilege boundaries, so this might not be a vulnerability in InfoPath. If no realistic scenarios exist for this problem in other products, then perhaps it should be excluded from CVE."  
  
[CVE-2005-4360] "The URL parser in Microsoft Internet Information Services (IIS) 5.1 on Windows XP Professional SP2 allows remote attackers to execute arbitrary code via multiple requests to "".dll"" followed by arguments such as ""~0"" through ""~9"", which causes ntdll.dll to produce a return value that is not correctly handled by IIS, as demonstrated using ""/\_vti\_bin/.dll/\*/~0"". NOTE: the consequence was originally believed to be only a denial of service (application crash and reboot)."  
  
[CVE-2005-4560] The Windows Graphical Device Interface library (GDI32.DLL) in Microsoft Windows allows remote attackers to execute arbitrary code via a Windows Metafile (WMF) format image with a crafted SETABORTPROC GDI Escape function call, related to the Windows Picture and Fax Viewer (SHIMGVW.DLL), a different vulnerability than CVE-2005-2123 and CVE-2005-2124, and as originally discovered in the wild on unionseek.com.  
  
[CVE-2005-4717] Microsoft Internet Explorer 6.0 on Windows NT 4.0 SP6a, Windows 2000 SP4, Windows XP SP1, Windows XP SP2, and Windows Server 2003 SP1 allows remote attackers to cause a denial of service (client crash) via a certain combination of a malformed HTML file and a CSS file that triggers a null dereference, probably related to rendering of a DIV element that contains a malformed IMG tag, as demonstrated by IEcrash.htm and IEcrash.rar.  
  
[CVE-2006-0005] Buffer overflow in the plug-in for Microsoft Windows Media Player (WMP) 9 and 10, when used in browsers other than Internet Explorer and set as the default application to handle media files, allows remote attackers to execute arbitrary code via HTML with an EMBED element containing a long src attribute.  
  
[CVE-2006-0006] Heap-based buffer overflow in the bitmap processing routine in Microsoft Windows Media Player 7.1 on Windows 2000 SP4, Media Player 9 on Windows 2000 SP4 and XP SP1, and Media Player 10 on XP SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted bitmap (.BMP) file that specifies a size of 0 but contains additional data.  
  
[CVE-2006-0008] "The ShellAbout API call in Korean Input Method Editor (IME) in Korean versions of Microsoft Windows XP SP1 and SP2, Windows Server 2003 up to SP1, and Office 2003, allows local users to gain privileges by launching the ""shell about dialog box"" and clicking the ""End-User License Agreement"" link, which executes Notepad with the privileges of the program that displays the about box."  
  
[CVE-2006-0010] Heap-based buffer overflow in T2EMBED.DLL in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to SP1, Windows 98, and Windows ME allows remote attackers to execute arbitrary code via an e-mail message or web page with a crafted Embedded Open Type (EOT) web font that triggers the overflow during decompression.  
  
[CVE-2006-0012] "Unspecified vulnerability in Windows Explorer in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via attack vectors involving COM objects and ""crafted files and directories,"" aka the ""Windows Shell Vulnerability."""  
  
[CVE-2006-0014] "Buffer overflow in Microsoft Outlook Express 5.5 and 6 allows remote attackers to execute arbitrary code via a crafted Windows Address Book (WAB) file containing ""certain Unicode strings"" and modified length values."  
  
[CVE-2006-0020] "An unspecified Microsoft WMF parsing application, as used in Internet Explorer 5.01 SP4 on Windows 2000 SP4, and 5.5 SP2 on Windows Millennium, and possibly other versions, allows attackers to cause a denial of service (crash) and possibly execute code via a crafted WMF file with a manipulated WMF header size, possibly involving an integer overflow, a different vulnerability than CVE-2005-4560, and aka ""WMF Image Parsing Memory Corruption Vulnerability."""  
  
[CVE-2006-0021] "Microsoft Windows XP SP1 and SP2, and Server 2003 up to SP1, allows remote attackers to cause a denial of service (hang) via an IGMP packet with an invalid IP option, aka the ""IGMP v3 DoS Vulnerability."""  
  
[CVE-2006-0023] "Microsoft Windows XP SP1 and SP2 before August 2004, and possibly other operating systems and versions, uses insecure default ACLs that allow the Authenticated Users group to gain privileges by modifying critical configuration information for the (1) Simple Service Discovery Protocol (SSDP), (2) Universal Plug and Play Device Host (UPnP), (3) NetBT, (4) SCardSvr, (5) DHCP, and (6) DnsCache services, aka ""Permissive Windows Services DACLs."" NOTE: the NetBT, SCardSvr, DHCP, DnsCache already require privileged access to exploit."  
  
[CVE-2006-0025] Stack-based buffer overflow in Microsoft Windows Media Player 9 and 10 allows remote attackers to execute arbitrary code via a PNG image with a large chunk size.  
  
[CVE-2006-0032] Cross-site scripting (XSS) vulnerability in the Indexing Service in Microsoft Windows 2000, XP, and Server 2003, when the Encoding option is set to Auto Select, allows remote attackers to inject arbitrary web script or HTML via a UTF-7 encoded URL, which is injected into an error message whose charset is set to UTF-7.  
  
[CVE-2006-0143] Microsoft Windows Graphics Rendering Engine (GRE) allows remote attackers to corrupt memory and cause a denial of service (crash) via a WMF file containing (1) ExtCreateRegion or (2) ExtEscape function calls with arguments with inconsistent lengths.  
  
[CVE-2006-0561] Cisco Secure Access Control Server (ACS) 3.x for Windows stores ACS administrator passwords and the master key in the registry with insecure permissions, which allows local users and remote administrators to decrypt the passwords by using Microsoft's cryptographic API functions to obtain the plaintext version of the master key.  
  
[CVE-2006-0753] Memory leak in Microsoft Internet Explorer 6 for Windows XP Service Pack 2 allows remote attackers to cause a denial of service (memory consumption) via JavaScript that uses setInterval to repeatedly call a function to set the value of window.status.  
  
[CVE-2006-0988] The default configuration of the DNS Server service on Windows Server 2003 and Windows 2000, and the Microsoft DNS Server service on Windows NT 4.0, allows recursive queries and provides additional delegation information to arbitrary IP addresses, which allows remote attackers to cause a denial of service (traffic amplification) via DNS queries with spoofed source IP addresses.  
  
[CVE-2006-1184] Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0, 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to cause a denial of service (crash) via a BuildContextW request with a large (1) UuidString or (2) GuidIn of a certain length, which causes an out-of-range memory access, aka the MSDTC Denial of Service Vulnerability. NOTE: this is a variant of CVE-2005-2119.  
  
[CVE-2006-1300] "Microsoft .NET framework 2.0 (ASP.NET) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to bypass access restrictions via unspecified ""URL paths"" that can access Application Folder objects ""explicitly by name."""  
  
[CVE-2006-1311] "The RichEdit component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1  
[CVE-2006-1313] "Microsoft JScript 5.1, 5.5, and 5.6 on Windows 2000 SP4, and 5.6 on Windows XP, Server 2003, Windows 98 and Windows Me, will ""release objects early"" in certain cases, which results in memory corruption and allows remote attackers to execute arbitrary code."  
  
[CVE-2006-1314] Heap-based buffer overflow in the Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to execute arbitrary code via crafted first-class Mailslot messages that triggers memory corruption and bypasses size restrictions on second-class Mailslot messages.  
  
[CVE-2006-1315] "The Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka ""SMB Information Disclosure Vulnerability."""  
  
[CVE-2006-1475] Windows Firewall in Microsoft Windows XP SP2 does not produce application alerts when an application is executed using the NTFS Alternate Data Streams (ADS) filename:stream syntax, which might allow local users to launch a Trojan horse attack in which the victim does not obtain the alert that Windows Firewall would have produced for a non-ADS file.  
  
[CVE-2006-1476] "Windows Firewall in Microsoft Windows XP SP2 produces incorrect application block alerts when the application filename is "".exe"" (with no characters before the "".""), which might allow local user-assisted users to trick a user into unblocking a Trojan horse program, as demonstrated by a malicious "".exe"" program in a folder named ""Internet Explorer,"" which triggers a question about whether to unblock the ""Internet Explorer"" program."  
  
[CVE-2006-1510] Buffer overflow in calloc.c in the Microsoft Windows XP SP2 ntdll.dll system library, when used by the ILDASM disassembler in the Microsoft .NET 1.0 and 1.1 SDK, might allow user-assisted attackers to execute arbitrary code via a crafted .dll file with a large static method.  
  
[CVE-2006-1591] Heap-based buffer overflow in Microsoft Windows Help winhlp32.exe allows user-assisted attackers to execute arbitrary code via crafted embedded image data in a .hlp file.  
  
[CVE-2006-1651] "\*\* DISPUTED \*\* Microsoft ISA Server 2004 allows remote attackers to bypass certain filtering rules, including ones for (1) ICMP and (2) TCP, via IPv6 packets. NOTE: An established researcher has disputed this issue, saying that ""Neither ISA Server 2004 nor Windows 2003 Basic Firewall support IPv6 filtering ... This is different network protocol."""  
  
[CVE-2006-1654] Directory traversal vulnerability in the HP Color LaserJet 2500 Toolbox and Color LaserJet 4600 Toolbox on Microsoft Windows before 20060402 allows remote attackers to read arbitrary files via a .. (dot dot) in an HTTP GET request to TCP port 5225.  
  
[CVE-2006-2056] "Argument injection vulnerability in Internet Explorer 6 for Windows XP SP2 allows user-assisted remote attackers to modify command line arguments to an invoked mail client via "" (double quote) characters in a mailto: scheme handler, as demonstrated by launching Microsoft Outlook with an arbitrary filename as an attachment. NOTE: it is not clear whether this issue is implementation-specific or a problem in the Microsoft API."  
  
[CVE-2006-2094] "Microsoft Internet Explorer before Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, when Prompt is configured in Security Settings, uses modal dialogs to verify that a user wishes to run an ActiveX control or perform other risky actions, which allows user-assisted remote attackers to construct a race condition that tricks a user into clicking an object or pressing keys that are actually applied to a ""Yes"" approval for executing the control."  
  
[CVE-2006-2218] "Unspecified vulnerability in Internet Explorer 6.0 on Microsoft Windows XP SP2 allows remote attackers to execute arbitrary code via ""exceptional conditions"" that trigger memory corruption, as demonstrated using an exception handler and nested object tags, a variant of CVE-2006-1992."  
  
[CVE-2006-2334] The RtlDosPathNameToNtPathName\_U API function in NTDLL.DLL in Microsoft Windows 2000 SP4 and XP SP2 does not properly convert DOS style paths with trailing spaces into NT style paths, which allows context-dependent attackers to create files that cannot be accessed through the expected DOS path or prevent access to other similarly named files in the same directory, which prevents those files from being detected or disinfected by certain anti-virus and anti-spyware software.  
  
[CVE-2006-2372] Buffer overflow in the DHCP Client service for Microsoft Windows 2000 SP4, Windows XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via a crafted DHCP response.  
  
[CVE-2006-2373] "The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to execute arbitrary code by calling the MrxSmbCscIoctlOpenForCopyChunk function with the METHOD\_NEITHER method flag and an arbitrary address, possibly for kernel memory, aka the ""SMB Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2006-2374] "The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to cause a denial of service (hang) by calling the MrxSmbCscIoctlCloseForCopyChunk with the file handle of the shadow device, which results in a deadlock, aka the ""SMB Invalid Handle Vulnerability."""  
  
[CVE-2006-2376] Integer overflow in the PolyPolygon function in Graphics Rendering Engine on Microsoft Windows 98 and Me allows remote attackers to execute arbitrary code via a Windows Metafile (WMF) or EMF image with a sum of entries in the vertext counts array and number of polygons that triggers a heap-based buffer overflow.  
  
[CVE-2006-2378] Buffer overflow in the ART Image Rendering component (jgdw400.dll) in Microsoft Windows XP SP1 and Sp2, Server 2003 SP1 and earlier, and Windows 98 and Me allows remote attackers to execute arbitrary code via a crafted ART image that causes heap corruption.  
  
[CVE-2006-2379] Buffer overflow in the TCP/IP Protocol driver in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via unknown vectors related to IP source routing.  
  
[CVE-2006-2386] Unspecified vulnerability in Microsoft Outlook Express 6 and earlier allows remote attackers to execute arbitrary code via a crafted contact record in a Windows Address Book (WAB) file.  
  
[CVE-2006-2766] Buffer overflow in INETCOMM.DLL, as used in Microsoft Internet Explorer 6.0 through 6.0 SP2, Windows Explorer, Outlook Express 6, and possibly other programs, allows remote user-assisted attackers to cause a denial of service (application crash) via a long mhtml URI in the URL value in a URL file.  
  
[CVE-2006-3209] \*\* DISPUTED \*\* The Task scheduler (at.exe) on Microsoft Windows XP spawns each scheduled process with SYSTEM permissions, which allows local users to gain privileges. NOTE: this issue has been disputed by third parties, who state that the Task scheduler is limited to the Administrators group by default upon installation.  
  
[CVE-2006-3440] "Buffer overflow in the Winsock API in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via unknown vectors, aka ""Winsock Hostname Vulnerability."""  
  
[CVE-2006-3441] Buffer overflow in the DNS Client service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted record response. NOTE: while MS06-041 implies that there is a single issue, there are multiple vectors, and likely multiple vulnerabilities, related to (1) a heap-based buffer overflow in a DNS server response to the client, (2) a DNS server response with malformed ATMA records, and (3) a length miscalculation in TXT, HINFO, X25, and ISDN records.  
  
[CVE-2006-3442] Unspecified vulnerability in Pragmatic General Multicast (PGM) in Microsoft Windows XP SP2 and earlier allows remote attackers to execute arbitrary code via a crafted multicast message.  
  
[CVE-2006-3443] "Untrusted search path vulnerability in Winlogon in Microsoft Windows 2000 SP4, when SafeDllSearchMode is disabled, allows local users to gain privileges via a malicious DLL in the UserProfile directory, aka ""User Profile Elevation of Privilege Vulnerability."""  
  
[CVE-2006-3444] "Unspecified vulnerability in the kernel in Microsoft Windows 2000 SP4, probably a buffer overflow, allows local users to obtain privileges via unspecified vectors involving an ""unchecked buffer."""  
  
[CVE-2006-3445] Integer overflow in the ReadWideString function in agentdpv.dll in Microsoft Agent on Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via a large length value in an .ACF file, which results in a heap-based buffer overflow.  
  
[CVE-2006-3448] Buffer overflow in the Step-by-Step Interactive Training in Microsoft Windows 2000 SP4, XP SP2 and Professional, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a long Syllabus string in crafted bookmark link files (cbo, cbl, or .cbm), a different issue than CVE-2005-1212.  
  
[CVE-2006-3471] Microsoft Internet Explorer 6 on Windows XP allows remote attackers to cause a denial of service (crash) via a table with a frameset as a child, which triggers a null dereference, as demonstrated using the appendChild method.  
  
[CVE-2006-3510] The Remote Data Service Object (RDS.DataControl) in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (crash) via a series of operations that result in an invalid length calculation when using SysAllocStringLen, then triggers a buffer over-read.  
  
[CVE-2006-3643] "Cross-site scripting (XSS) vulnerability in Internet Explorer 5.01 and 6 in Microsoft Windows 2000 SP4 permits access to local ""HTML-embedded resource files"" in the Microsoft Management Console (MMC) library, which allows remote authenticated users to execute arbitrary commands, aka ""MMC Redirect Cross-Site Scripting Vulnerability."""  
  
[CVE-2006-3648] "Unspecified vulnerability in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 and 2003 SP1, allows remote attackers to execute arbitrary code via unspecified vectors involving unhandled exceptions, memory resident applications, and incorrectly ""unloading chained exception."""  
  
[CVE-2006-3730] Integer overflow in Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a 0x7fffffff argument to the setSlice method on a WebViewFolderIcon ActiveX object, which leads to an invalid memory copy.  
  
[CVE-2006-3869] Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060824, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL on a website that uses HTTP 1.1 compression.  
  
[CVE-2006-3873] Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060912, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL in a GZIP-encoded website that was the target of an HTTP redirect, due to an incomplete fix for CVE-2006-3869.  
  
[CVE-2006-3880] "\*\* DISPUTED \*\* Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Small Business Server 2003 allow remote attackers to cause a denial of service (IP stack hang) via a continuous stream of packets on TCP port 135 that have incorrect TCP header checksums and random numbers in certain TCP header fields, as demonstrated by the Achilles Windows Attack Tool. NOTE: the researcher reports that the Microsoft Security Response Center has stated ""Our investigation which has included code review, review of the TCPDump, and attempts on reproing the issue on multiple fresh installs of various Windows Operating Systems have all resulted in non confirmation."""  
  
[CVE-2006-3897] Stack overflow in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (application crash) by creating an NMSA.ASFSourceMediaDescription.1 ActiveX object with a long dispValue property.  
  
[CVE-2006-3898] Microsoft Internet Explorer 6.0 on Windows XP SP2 allows remote attackers to cause a denial of service (application crash) by calling the Click method of the Internet.HHCtrl.1 ActiveX object before initializing the URL, which triggers a null dereference.  
  
[CVE-2006-3899] Microsoft Internet Explorer 6.0 on Windows XP SP2 allows remote attackers to cause a denial of service (application crash) by calling the stringToBinary function of the CEnroll.CEnroll.2 ActiveX object with a long second argument, which triggers an invalid memory access inside the SysAllocStringLen function.  
  
[CVE-2006-3915] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by iterating over any native function, as demonstrated with the window.alert function, which triggers a null dereference.  
  
[CVE-2006-3942] "The server driver (srv.sys) in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to cause a denial of service (system crash) via an SMB\_COM\_TRANSACTION SMB message that contains a string without null character termination, which leads to a NULL dereference in the ExecuteTransaction function, possibly related to an ""SMB PIPE,"" aka the ""Mailslot DOS"" vulnerability. NOTE: the name ""Mailslot DOS"" was derived from incomplete initial research  
[CVE-2006-3943] Stack-based buffer overflow in NDFXArtEffects in Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) via long (1) RGBExtraColor, (2) RGBForeColor, and (3) RGBBackColor properties.  
  
[CVE-2006-3944] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) via a (1) Forms.ListBox.1 or (2) Forms.ListBox.1 object with the ListWidth property set to (a) 0x7fffffff, which triggers an integer overflow exception, or to (b) 0x7ffffffe, which triggers a null dereference.  
  
[CVE-2006-3992] Unspecified vulnerability in the Centrino (1) w22n50.sys, (2) w22n51.sys, (3) w29n50.sys, and (4) w29n51.sys Microsoft Windows drivers for Intel 2200BG and 2915ABG PRO/Wireless Network Connection before 10.5 with driver 9.0.4.16 allows remote attackers to execute arbitrary code via certain frames that trigger memory corruption.  
  
[CVE-2006-4066] The Graphical Device Interface Plus library (gdiplus.dll) in Microsoft Windows XP SP2 allows context-dependent attackers to cause a denial of service (application crash) via certain images that trigger a divide-by-zero error, as demonstrated by a (1) .ico file, (2) .png file that crashes MSN Messenger, and (3) .jpg file that crashes Internet Explorer. NOTE: another researcher has not been able to reproduce this issue.  
  
[CVE-2006-4071] Sign extension vulnerability in the createBrushIndirect function in the GDI library (gdi32.dll) in Microsoft Windows XP, Server 2003, and possibly other versions, allows user-assisted attackers to cause a denial of service (application crash) via a crafted WMF file.  
  
[CVE-2006-4128] Multiple heap-based buffer overflows in Symantec VERITAS Backup Exec for Netware Server Remote Agent for Windows Server 9.1 and 9.2 (all builds), Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1 (builds 10.1.325.6301, 10.1.326.1401, 10.1.326.2501, 10.1.326.3301, and 10.1.327.401), and Backup Exec for Windows Server and Remote Agent 9.1 (build 9.1.4691), 10.0 (builds 10.0.5484 and 10.0.5520), and 10.1 (build 10.1.5629) allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted RPC message.  
  
[CVE-2006-4138] Multiple unspecified vulnerabilities in Microsoft Windows Help File viewer (winhlp32.exe) allow user-assisted attackers to execute arbitrary code via crafted HLP files.  
  
[CVE-2006-4219] The Terminal Services COM object (tsuserex.dll) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by instantiating it as an ActiveX object in Internet Explorer 6.0 SP1 on Microsoft Windows 2003 EE SP1 CN.  
  
[CVE-2006-4495] Microsoft Internet Explorer allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code by instantiating certain Windows 2000 ActiveX COM Objects including (1) ciodm.dll, (2) myinfo.dll, (3) msdxm.ocx, and (4) creator.dll.  
  
[CVE-2006-4688] "Buffer overflow in Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via crafted messages, aka ""Client Service for NetWare Memory Corruption Vulnerability."""  
  
[CVE-2006-4689] "Unspecified vulnerability in the driver for the Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to cause a denial of service (hang and reboot) via has unknown attack vectors, aka ""NetWare Driver Denial of Service Vulnerability."""  
  
[CVE-2006-4692] "Argument injection vulnerability in the Windows Object Packager (packager.exe) in Microsoft Windows XP SP1 and SP2 and Server 2003 SP1 and earlier allows remote user-assisted attackers to execute arbitrary commands via a crafted file with a ""/"" (slash) character in the filename of the Command Line property, followed by a valid file extension, which causes the command before the slash to be executed, aka ""Object Packager Dialogue Spoofing Vulnerability."""  
  
[CVE-2006-4694] Unspecified vulnerability in PowerPoint in Microsoft Office 2000, Office XP and Office 2003 allows user-assisted attackers to execute arbitrary code via a crafted record in a PPT file, as exploited by malware such as Exploit:Win32/Controlppt.W, Exploit:Win32/Controlppt.X, and Exploit-PPT.d/Trojan.PPDropper.F. NOTE: it has been reported that the attack vector involves SlideShowWindows.View.GotoNamedShow.  
  
[CVE-2006-4696] "Unspecified vulnerability in the Server service in Microsoft Windows 2000 SP4, Server 2003 SP1 and earlier, and XP SP2 and earlier allows remote attackers to execute arbitrary code via a crafted packet, aka ""SMB Rename Vulnerability."""  
  
[CVE-2006-4702] Buffer overflow in the Windows Media Format Runtime in Microsoft Windows Media Player (WMP) 6.4 and Windows XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted Advanced Systems Format (ASF) file.  
  
[CVE-2006-4868] Stack-based buffer overflow in the Vector Graphics Rendering engine (vgx.dll), as used in Microsoft Outlook and Internet Explorer 6.0 on Windows XP SP2, and possibly other versions, allows remote attackers to execute arbitrary code via a Vector Markup Language (VML) file with a long fill parameter within a rect tag.  
  
[CVE-2006-5028] Directory traversal vulnerability in filemanager/filemanager.php in SWsoft Plesk 7.5 Reload and Plesk 7.6 for Microsoft Windows allows remote attackers to list arbitrary directories via a ../ (dot dot slash) in the file parameter in a chdir action.  
  
[CVE-2006-5270] Integer overflow in the Microsoft Malware Protection Engine (mpengine.dll), as used by Windows Live OneCare, Antigen, Defender, and Forefront Security, allows user-assisted remote attackers to execute arbitrary code via a crafted PDF file.  
  
[CVE-2006-5448] "The drmstor.dll ActiveX object in Microsoft Windows Digital Rights Management System (DRM) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long parameter to the StoreLicense function, which triggers ""memory corruption"" and possibly a buffer overflow."  
  
[CVE-2006-5583] "Buffer overflow in the SNMP Service in Microsoft Windows 2000 SP4, XP SP2, Server 2003, Server 2003 SP1, and possibly other versions allows remote attackers to execute arbitrary code via a crafted SNMP packet, aka ""SNMP Memory Corruption Vulnerability."""  
  
[CVE-2006-5584] The Remote Installation Service (RIS) in Microsoft Windows 2000 SP4 uses a TFTP server that allows anonymous access, which allows remote attackers to upload and overwrite arbitrary files to gain privileges on systems that use RIS.  
  
[CVE-2006-5585] "The Client-Server Run-time Subsystem in Microsoft Windows XP SP2 and Server 2003 allows local users to gain privileges via a crafted file manifest within an application, aka ""File Manifest Corruption Vulnerability."""  
  
[CVE-2006-5586] "The Graphics Rendering Engine in Microsoft Windows 2000 SP4 and XP SP2 allows local users to gain privileges via ""invalid application window sizes"" in layered application windows, aka the ""GDI Invalid Window Size Elevation of Privilege Vulnerability."""  
  
[CVE-2006-5614] Microsoft Windows NAT Helper Components (ipnathlp.dll) on Windows XP SP2, when Internet Connection Sharing is enabled, allows remote attackers to cause a denial of service (svchost.exe crash) via a malformed DNS query, which results in a null pointer dereference.  
  
[CVE-2006-5745] Unspecified vulnerability in the setRequestHeader method in the XMLHTTP (XML HTTP) ActiveX Control 4.0 in Microsoft XML Core Services 4.0 on Windows, when accessed by Internet Explorer, allows remote attackers to execute arbitrary code via crafted arguments that lead to memory corruption, a different vulnerability than CVE-2006-4685. NOTE: some of these details are obtained from third party information.  
  
[CVE-2006-5758] The Graphics Rendering Engine in Microsoft Windows 2000 through 2000 SP4 and Windows XP through SP2 maps GDI Kernel structures on a global shared memory section that is mapped with read-only permissions, but can be remapped by other processes as read-write, which allows local users to cause a denial of service (memory corruption and crash) and gain privileges by modifying the kernel structures.  
  
[CVE-2006-6134] Heap-based buffer overflow in the WMCheckURLScheme function in WMVCORE.DLL in Microsoft Windows Media Player (WMP) 10.00.00.4036 on Windows XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to cause a denial of service (application crash) and execute arbitrary code via a long HREF attribute, using an unrecognized protocol, in a REF element in an ASX PlayList file.  
  
[CVE-2006-6252] "Microsoft Windows Live Messenger 8.0 and earlier, when gestual emoticons are enabled, allows remote attackers to cause a denial of service (CPU consumption) via a long string composed of "":D"" sequences, which are interpreted as emoticons."  
  
[CVE-2006-6579] Microsoft Windows XP has weak permissions (FILE\_WRITE\_DATA and FILE\_READ\_DATA for Everyone) for %WINDIR%\pchealth\ERRORREP\QHEADLES, which allows local users to write and read files in this folder, as demonstrated by an ASP shell that has write access by IWAM\_machine and read access by IUSR\_Machine.  
  
[CVE-2006-6601] Windows Media Player 10.00.00.4036 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service via a .MID (MIDI) file with a malformed header chunk without any track chunks, possibly involving (1) number of tracks of (2) time division fields that are set to 0.  
  
[CVE-2006-6602] explorer.exe in Windows Explorer 6.00.2900.2180 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service via a crafted WMV file.  
  
[CVE-2006-6659] The Microsoft Office Outlook Recipient ActiveX control (ole32.dll) in Windows XP SP2 allows remote attackers to cause a denial of service (Internet Explorer 7 hang) via crafted HTML.  
  
[CVE-2006-6696] Double free vulnerability in Microsoft Windows 2000, XP, 2003, and Vista allows local users to gain privileges by calling the MessageBox function with a MB\_SERVICE\_NOTIFICATION message with crafted data, which sends a HardError message to Client/Server Runtime Server Subsystem (CSRSS) process, which is not properly handled when invoking the UserHardError and GetHardErrorText functions in WINSRV.DLL.  
  
[CVE-2006-6753] Event Viewer (eventvwr.exe) in Microsoft Windows does not properly display log data that contains '%' (percent) characters, which might make it impossible to use Event Viewer to determine the actual data that triggered an event, and might produce long strings that are not properly handled by certain processes that rely on Event Viewer.  
  
[CVE-2006-6797] The Client Server Run-Time Subsystem (CSRSS) in Microsoft Windows allows local users to cause a denial of service (crash) or read arbitrary memory from csrss.exe via crafted arguments to the NtRaiseHardError function with status 0x50000018, a different vulnerability than CVE-2006-6696.  
  
[CVE-2006-6901] Unspecified vulnerability in the Bluetooth stack in Microsoft Windows allows remote attackers to gain administrative access (aka Remote Root) via unspecified vectors.  
  
[CVE-2006-6902] Unspecified vulnerability in the Bluetooth stack in Microsoft Windows Mobile Pocket PC edition allows remote attackers to gain administrative access (aka Remote Root) via unspecified vectors.  
  
[CVE-2006-7066] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by creating an object inside an iframe, deleting the frame by setting its location.href to about:blank, then accessing a property of the object within the deleted frame, which triggers a NULL pointer dereference. NOTE: it was later reported that 7.0.6000.16473 and earlier are also affected.  
  
[CVE-2006-7206] "Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by creating a ADODB.Recordset object and making a series of calls to the NextRecordset method with a long string argument, which causes an ""invalid memory access"" in the SysFreeString function, a different issue than CVE-2006-3510 and CVE-2006-3899."  
  
[CVE-2006-7210] Microsoft Windows 2000, XP, and Server 2003 allows remote attackers to cause a denial of service (cpu consumption) via a PNG image with crafted (1) Width and (2) Height values in the IHDR block.  
  
[CVE-2007-0024] "Integer overflow in the Vector Markup Language (VML) implementation (vgx.dll) in Microsoft Internet Explorer 5.01, 6, and 7 on Windows 2000 SP4, XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted web page that contains unspecified integer properties that cause insufficient memory allocation and trigger a buffer overflow, aka the ""VML Buffer Overrun Vulnerability."""  
  
[CVE-2007-0025] The MFC component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 and Visual Studio .NET 2000, 2002 SP1, 2003, and 2003 SP1 allows user-assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption. NOTE: this might be due to a stack-based buffer overflow in the AfxOleSetEditMenu function in MFC42u.dll.  
  
[CVE-2007-0026] The OLE Dialog component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 allows user-assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption.  
  
[CVE-2007-0038] "Stack-based buffer overflow in the animated cursor code in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a large length value in the second (or later) anih block of a RIFF .ANI, cur, or .ico file, which results in memory corruption when processing cursors, animated cursors, and icons, a variant of CVE-2005-0416, as originally demonstrated using Internet Explorer 6 and 7. NOTE: this might be a duplicate of CVE-2007-1765  
[CVE-2007-0040] "The LDAP service in Windows Active Directory in Microsoft Windows 2000 Server SP4, Server 2003 SP1 and SP2, Server 2003 x64 Edition and SP2, and Server 2003 for Itanium-based Systems SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted LDAP request with an unspecified number of ""convertible attributes."""  
  
[CVE-2007-0041] "The PE Loader service in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows remote attackers to execute arbitrary code via unspecified vectors involving an ""unchecked buffer"" and unvalidated message lengths, probably a buffer overflow."  
  
[CVE-2007-0042] "Interpretation conflict in ASP.NET in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows remote attackers to access configuration files and obtain sensitive information, and possibly bypass security mechanisms that try to constrain the final substring of a string, via %00 characters, related to use of %00 as a string terminator within POSIX functions but a data character within .NET strings, aka ""Null Byte Termination Vulnerability."""  
  
[CVE-2007-0043] "The Just In Time (JIT) Compiler service in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows user-assisted remote attackers to execute arbitrary code via unspecified vectors involving an ""unchecked buffer,"" probably a buffer overflow, aka "".NET JIT Compiler Vulnerability""."  
  
[CVE-2007-0045] "Multiple cross-site scripting (XSS) vulnerabilities in Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, for Mozilla Firefox, Microsoft Internet Explorer 6 SP1, Google Chrome, Opera 8.5.4 build 770, and Opera 9.10.8679 on Windows allow remote attackers to inject arbitrary JavaScript and conduct other attacks via a .pdf URL with a javascript: or res: URI with (1) FDF, (2) XML, and (3) XFDF AJAX parameters, or (4) an arbitrarily named name=URI anchor identifier, aka ""Universal XSS (UXSS)."""  
  
[CVE-2007-0064] Heap-based buffer overflow in Windows Media Format Runtime 7.1, 9, 9.5, 9.5 x64 Edition, 11, and Windows Media Services 9.1 for Microsoft Windows 2000, XP, Server 2003, and Vista allows user-assisted remote attackers to execute arbitrary code via a crafted Advanced Systems Format (ASF) file.  
  
[CVE-2007-0065] Heap-based buffer overflow in Object Linking and Embedding (OLE) Automation in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, Office 2004 for Mac, and Visual basic 6.0 SP6 allows remote attackers to execute arbitrary code via a crafted script request.  
  
[CVE-2007-0066] "The kernel in Microsoft Windows 2000 SP4, XP SP2, and Server 2003, when ICMP Router Discovery Protocol (RDP) is enabled, allows remote attackers to cause a denial of service via fragmented router advertisement ICMP packets that trigger an out-of-bounds read, aka ""Windows Kernel TCP/IP/ICMP Vulnerability."""  
  
[CVE-2007-0069] "Unspecified vulnerability in the kernel in Microsoft Windows XP SP2, Server 2003, and Vista allows remote attackers to cause a denial of service (CPU consumption) and possibly execute arbitrary code via crafted (1) IGMPv3 and (2) MLDv2 packets that trigger memory corruption, aka ""Windows Kernel TCP/IP/IGMPv3 and MLDv2 Vulnerability."""  
  
[CVE-2007-0084] \*\* DISPUTED \*\* Buffer overflow in the Windows NT Message Compiler (MC) 1.00.5239 on Microsoft Windows XP allows local users to gain privileges via a long MC-filename. NOTE: this issue has been disputed by a reliable third party who states that the compiler is not a privileged program, so privilege boundaries cannot be crossed.  
  
[CVE-2007-0210] "The Window Image Acquisition (WIA) Service in Microsoft Windows XP SP2 allows local users to gain privileges via unspecified vectors involving an ""unchecked buffer,"" probably a buffer overflow."  
  
[CVE-2007-0211] "The hardware detection functionality in the Windows Shell in Microsoft Windows XP SP2 and Professional, and Server 2003 SP1 allows local users to gain privileges via an unvalidated parameter to a function related to the ""detection and registration of new hardware."""  
  
[CVE-2007-0214] The HTML Help ActiveX control (Hhctrl.ocx) in Microsoft Windows 2000 SP3, XP SP2 and Professional, 2003 SP1 allows remote attackers to execute arbitrary code via unspecified functions, related to uninitialized parameters.  
  
[CVE-2007-0351] Microsoft Windows XP and Windows Server 2003 do not properly handle user logoff, which might allow local users to gain the privileges of a previous system user, possibly related to user profile unload failure. NOTE: it is not clear whether this is an issue in Windows itself, or an interaction with another product. The issue might involve ZoneAlarm not being able to terminate processes when it cannot prompt the user.  
  
[CVE-2007-0562] Windows Explorer (explorer.exe) 6.0.2900.2180 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted .avi file, which triggers the crash when the user right clicks on the file.  
  
[CVE-2007-0612] "Multiple ActiveX controls in Microsoft Windows 2000, XP, 2003, and Vista allows remote attackers to cause a denial of service (Internet Explorer crash) by accessing the bgColor, fgColor, linkColor, alinkColor, vlinkColor, or defaultCharset properties in the (1) giffile, (2) htmlfile, (3) jpegfile, (4) mhtmlfile, (5) ODCfile, (6) pjpegfile, (7) pngfile, (8) xbmfile, (9) xmlfile, (10) xslfile, or (11) wdfile objects in (a) mshtml.dll  
[CVE-2007-0675] A certain ActiveX control in sapi.dll (aka the Speech API) in Speech Components in Microsoft Windows Vista, when the Speech Recognition feature is enabled, allows user-assisted remote attackers to delete arbitrary files, and conduct other unauthorized activities, via a web page with an embedded sound object that contains voice commands to an enabled microphone, allowing for interaction with Windows Explorer.  
  
[CVE-2007-0811] Microsoft Internet Explorer 6.0 SP1 on Windows 2000, and 6.0 SP2 on Windows XP, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an HTML document containing a certain JavaScript for loop with an empty loop body, possibly involving getElementById.  
  
[CVE-2007-0843] The ReadDirectoryChangesW API function on Microsoft Windows 2000, XP, Server 2003, and Vista does not check permissions for child objects, which allows local users to bypass permissions by opening a directory with LIST (READ) access and using ReadDirectoryChangesW to monitor changes of files that do not have LIST permissions, which can be leveraged to determine filenames, access times, and other sensitive information.  
  
[CVE-2007-0878] "Unspecified vulnerability in Microsoft Internet Explorer on Windows Mobile 5.0 allows remote attackers to cause a denial of service (loss of browser and other device functionality) via a malformed WML page, related to an ""overflow state."" NOTE: it is possible that this issue is related to CVE-2007-0685."  
  
[CVE-2007-0942] "Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-0944] "Unspecified vulnerability in the CTableCol::OnPropertyChange method in Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-0945] "Microsoft Internet Explorer 6 SP1 on Windows 2000 SP4  
[CVE-2007-0946] "Unspecified vulnerability in Microsoft Internet Explorer 7 on Windows XP SP2, Windows Server 2003 SP1 or SP2, or Windows Vista allows remote attackers to execute arbitrary code via crafted HTML objects, which results in memory corruption, aka the first of two ""HTML Objects Memory Corruption Vulnerabilities"" and a different issue than CVE-2007-0947."  
  
[CVE-2007-0947] "Use-after-free vulnerability in Microsoft Internet Explorer 7 on Windows XP SP2, Windows Server 2003 SP1 or SP2, or Windows Vista allows remote attackers to execute arbitrary code via crafted HTML objects, resulting in accessing deallocated memory of CMarkup objects, aka the second of two ""HTML Objects Memory Corruption Vulnerabilities"" and a different issue than CVE-2007-0946."  
  
[CVE-2007-1070] Multiple stack-based buffer overflows in Trend Micro ServerProtect for Windows and EMC 5.58, and for Network Appliance Filer 5.61 and 5.62, allow remote attackers to execute arbitrary code via crafted RPC requests to TmRpcSrv.dll that trigger overflows when calling the (1) CMON\_NetTestConnection, (2) CMON\_ActiveUpdate, and (3) CMON\_ActiveRollback functions in (a) StCommon.dll, and (4) ENG\_SetRealTimeScanConfigInfo and (5) ENG\_SendEMail functions in (b) eng50.dll.  
  
[CVE-2007-1090] Microsoft Windows Explorer on Windows XP and 2003 allows remote user-assisted attackers to cause a denial of service (crash) via a malformed WMF file, which triggers the crash when the user browses the folder.  
  
[CVE-2007-1204] Stack-based buffer overflow in the Universal Plug and Play (UPnP) service in Microsoft Windows XP SP2 allows remote attackers on the same subnet to execute arbitrary code via crafted HTTP headers in request or notification messages, which trigger memory corruption.  
  
[CVE-2007-1205] Unspecified vulnerability in Microsoft Agent (msagent\agentsvr.exe) in Windows 2000 SP4, XP SP2, and Server 2003, 2003 SP1, and 2003 SP2 allows remote attackers to execute arbitrary code via crafted URLs, which result in memory corruption.  
  
[CVE-2007-1206] "The Virtual DOS Machine (VDM) in the Windows Kernel in Microsoft Windows NT 4.0  
[CVE-2007-1209] "Use-after-free vulnerability in the Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Vista does not properly handle connection resources when starting and stopping processes, which allows local users to gain privileges by opening and closing multiple ApiPort connections, which leaves a ""dangling pointer"" to a process data structure."  
  
[CVE-2007-1211] "Unspecified kernel GDI functions in Microsoft Windows 2000 SP4  
[CVE-2007-1212] "Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4  
[CVE-2007-1213] The TrueType Fonts rasterizer in Microsoft Windows 2000 SP4 allows local users to gain privileges via crafted TrueType fonts, which result in an uninitialized function pointer.  
  
[CVE-2007-1215] "Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4  
[CVE-2007-1347] Microsoft Windows Explorer on Windows 2000 SP4 FR and XP SP2 FR, and possibly other versions and platforms, allows remote attackers to cause a denial of service (memory corruption and crash) via an Office file with crafted document summary information, which causes an error in Ole32.dll.  
  
[CVE-2007-1492] winmm.dll in Microsoft Windows XP allows user-assisted remote attackers to cause a denial of service (infinite loop) via a large cch argument value to the mmioRead function, as demonstrated by a crafted WAV file.  
  
[CVE-2007-1499] "Microsoft Internet Explorer 7.0 on Windows XP and Vista allows remote attackers to conduct phishing attacks and possibly execute arbitrary code via a res: URI to navcancl.htm with an arbitrary URL as an argument, which displays the URL in the location bar of the ""Navigation Canceled"" page and injects the script into the ""Refresh the page"" link, aka Navigation Cancel Page Spoofing Vulnerability."""  
  
[CVE-2007-1512] "Stack-based buffer overflow in the AfxOleSetEditMenu function in the MFC component in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 Gold and SP1, and Visual Studio .NET 2002 Gold and SP1, and 2003 Gold and SP1 allows user-assisted remote attackers to have an unknown impact (probably crash) via an RTF file with a malformed OLE object, which results in writing two 0x00 characters past the end of szBuffer, aka the ""MFC42u.dll Off-by-Two Overflow."" NOTE: this issue is due to an incomplete patch (MS07-012) for CVE-2007-0025."  
  
[CVE-2007-1527] "The LLTD Mapper in Microsoft Windows Vista does not verify that an IP address in a TLV type 0x07 field in a HELLO packet corresponds to a valid IP address for the local network, which allows remote attackers to trick users into communicating with an external host by sending a HELLO packet with the MW characteristic and a spoofed TLV type 0x07 field, aka the ""Spoof and Management URL IP Redirect"" attack."  
  
[CVE-2007-1528] "The LLTD Mapper in Microsoft Windows Vista allows remote attackers to spoof hosts, and nonexistent bridge relationships, into the network topology map by using a MAC address that differs from the MAC address provided in the Real Source field of the LLTD BASE header of a HELLO packet, aka the ""Spoof on Bridge"" attack."  
  
[CVE-2007-1529] "The LLTD Responder in Microsoft Windows Vista does not send the Mapper a response to a DISCOVERY packet if another host has sent a spoofed response first, which allows remote attackers to spoof arbitrary hosts via a network-based race condition, aka the ""Total Spoof"" attack."  
  
[CVE-2007-1530] The LLTD Mapper in Microsoft Windows Vista does not properly gather responses to EMIT packets, which allows remote attackers to cause a denial of service (mapping failure) by omitting an ACK response, which triggers an XML syntax error.  
  
[CVE-2007-1531] Microsoft Windows XP and Vista overwrites ARP table entries included in gratuitous ARP, which allows remote attackers to cause a denial of service (loss of network access) by sending a gratuitous ARP for the address of the Vista host.  
  
[CVE-2007-1532] The neighbor discovery implementation in Microsoft Windows Vista allows remote attackers to conduct a redirect attack by (1) responding to queries by sending spoofed Neighbor Advertisements or (2) blindly sending Neighbor Advertisements.  
  
[CVE-2007-1533] The Teredo implementation in Microsoft Windows Vista uses the same nonce for communication with different UDP ports within a solicitation session, which makes it easier for remote attackers to spoof the nonce through brute force attacks.  
  
[CVE-2007-1534] DFSR.exe in Windows Meeting Space in Microsoft Windows Vista remains available for remote connections on TCP port 5722 for 2 minutes after Windows Meeting Space is closed, which allows remote attackers to have an unknown impact by connecting to this port during the time window.  
  
[CVE-2007-1535] Microsoft Windows Vista establishes a Teredo address without user action upon connection to the Internet, contrary to documentation that Teredo is inactive without user action, which increases the attack surface and allows remote attackers to communicate via Teredo.  
  
[CVE-2007-1537] \Device\NdisTapi (NDISTAPI.sys) in Microsoft Windows XP SP2 and 2003 SP1 uses weak permissions, which allows local users to write to the device and cause a denial of service, as demonstrated by using an IRQL to acquire a spinlock on paged memory via the NdisTapiDispatch function.  
  
[CVE-2007-1644] The dynamic DNS update mechanism in the DNS Server service on Microsoft Windows does not properly authenticate clients in certain deployments or configurations, which allows remote attackers to change DNS records for a web proxy server and conduct man-in-the-middle (MITM) attacks on web traffic, conduct pharming attacks by poisoning DNS records, and cause a denial of service (erroneous name resolution).  
  
[CVE-2007-1645] Buffer overflow in FutureSoft TFTP Server 2000 on Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via a long request on UDP port 69. NOTE: this issue might overlap CVE-2006-4781 or CVE-2005-1812.  
  
[CVE-2007-1658] Windows Mail in Microsoft Windows Vista might allow user-assisted remote attackers to execute certain programs via a link to a (1) local file or (2) UNC share pathname in which there is a directory with the same base name as an executable program at the same level, as demonstrated using C:/windows/system32/winrm (winrm.cmd) and migwiz (migwiz.exe).  
  
[CVE-2007-1692] The default configuration of Microsoft Windows uses the Web Proxy Autodiscovery Protocol (WPAD) without static WPAD entries, which might allow remote attackers to intercept web traffic by registering a proxy server using WINS or DNS, then responding to WPAD requests, as demonstrated using Internet Explorer. NOTE: it could be argued that if an attacker already has control over WINS/DNS, then web traffic could already be intercepted by modifying WINS or DNS records, so this would not cross privilege boundaries and would not be a vulnerability. It has also been reported that DHCP is an alternate attack vector.  
  
[CVE-2007-1763] The ATI kernel driver (atikmdag.sys) in Microsoft Windows Vista allows user-assisted remote attackers to cause a denial of service (crash) via a crafted JPG image, as demonstrated by a slideshow, possibly due to a buffer overflow.  
  
[CVE-2007-1765] "Unspecified vulnerability in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a malformed ANI file, which results in memory corruption when processing cursors, animated cursors, and icons, a similar issue to CVE-2005-0416, as originally demonstrated using Internet Explorer 6 and 7. NOTE: this issue might be a duplicate of CVE-2007-0038  
[CVE-2007-1912] Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.  
  
[CVE-2007-1946] Integer overflow in Windows Explorer in Microsoft Windows XP SP1 might allow user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large width dimension in a crafted BMP image, as demonstrated by w4intof.bmp.  
  
[CVE-2007-1973] Race condition in the Virtual DOS Machine (VDM) in the Windows Kernel in Microsoft Windows NT 4.0 allows local users to modify memory and gain privileges via the temporary \Device\PhysicalMemory section handle, a related issue to CVE-2007-1206.  
  
[CVE-2007-2217] Kodak Image Viewer in Microsoft Windows 2000 SP4, and in some cases XP SP2 and Server 2003 SP1 and SP2, allows remote attackers to execute arbitrary code via crafted image files that trigger memory corruption, as demonstrated by a certain .tif (TIFF) file.  
  
[CVE-2007-2218] Unspecified vulnerability in the Windows Schannel Security Package for Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2, allows remote servers to execute arbitrary code or cause a denial of service via crafted digital signatures that are processed during an SSL handshake.  
  
[CVE-2007-2219] Unspecified vulnerability in the Win32 API on Microsoft Windows 2000, XP SP2, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via certain parameters to an unspecified function.  
  
[CVE-2007-2221] "Unspecified vulnerability in the mdsauth.dll COM object in Microsoft Windows Media Server in the Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-2224] Object linking and embedding (OLE) Automation, as used in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Office 2004 for Mac, and Visual Basic 6.0 allows remote attackers to execute arbitrary code via the substringData method on a TextNode object, which causes an integer overflow that leads to a buffer overflow.  
  
[CVE-2007-2225] "A component in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle certain HTTP headers when processing MHTML protocol URLs, which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka ""URL Parsing Cross Domain Information Disclosure Vulnerability."""  
  
[CVE-2007-2227] "The MHTML protocol handler in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle Content-Disposition ""notifications,"" which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka ""Content Disposition Parsing Cross Domain Information Disclosure Vulnerability."""  
  
[CVE-2007-2229] "Microsoft Windows Vista uses insecure default permissions for unspecified ""local user information data stores"" in the registry and the file system, which allows local users to obtain sensitive information such as administrative passwords, aka ""Permissive User Information Store ACLs Information Disclosure Vulnerability."""  
  
[CVE-2007-2237] Microsoft Windows Graphics Device Interface (GDI+, GdiPlus.dll) allows context-dependent attackers to cause a denial of service (crash) via an ICO file with an InfoHeader containing a Height of zero, which triggers a divide-by-zero error.  
  
[CVE-2007-2374] Unspecified vulnerability in Microsoft Windows 2000, XP, and Server 2003 allows user-assisted remote attackers to execute arbitrary code via unspecified vectors. NOTE: this information is based upon a vague pre-advisory with no actionable information. However, the advisory is from a reliable source.  
  
[CVE-2007-2528] Buffer overflow in AgRpcCln.dll for Trend Micro ServerProtect 5.58 for Windows before Security Patch 3 Build 1176 allows remote attackers to execute arbitrary code via unknown vectors related to RPC requests. NOTE: this is probably a different vulnerability than CVE-2007-2508.  
  
[CVE-2007-2581] "Multiple cross-site scripting (XSS) vulnerabilities in Microsoft Windows SharePoint Services 3.0 for Windows Server 2003 and Office SharePoint Server 2007 allow remote attackers to inject arbitrary web script or HTML via the PATH\_INFO (query string) in ""every main page,"" as demonstrated by default.aspx."  
  
[CVE-2007-2593] The Terminal Server in Microsoft Windows 2003 Server, when using TLS, allows remote attackers to bypass SSL and self-signed certificate requirements, downgrade the server security, and possibly conduct man-in-the-middle attacks via unspecified vectors, as demonstrated using the Remote Desktop Protocol (RDP) 6.0 client. NOTE: a third party claims that the vendor may have fixed this in approximately 2006.  
  
[CVE-2007-2729] Comodo Firewall Pro 2.4.18.184 and Comodo Personal Firewall 2.3.6.81, and probably older Comodo Firewall versions, do not properly test for equivalence of process identifiers for certain Microsoft Windows API functions in the NT kernel 5.0 and greater, which allows local users to call these functions, and bypass firewall rules or gain privileges, via a modified identifier that is one, two, or three greater than the canonical identifier.  
  
[CVE-2007-2730] Check Point ZoneAlarm Pro before 6.5.737.000 does not properly test for equivalence of process identifiers for certain Microsoft Windows API functions in the NT kernel 5.0 and greater, which allows local users to call these functions, and bypass firewall rules or gain privileges, via a modified identifier that is one, two, or three greater than the canonical identifier.  
  
[CVE-2007-2815] "The ""hit-highlighting"" functionality in webhits.dll in Microsoft Internet Information Services (IIS) Web Server 5.0 only uses Windows NT ACL configuration, which allows remote attackers to bypass NTLM and basic authentication mechanisms and access private web directories via the CiWebhitsfile parameter to null.htw."  
  
[CVE-2007-2954] Multiple stack-based buffer overflows in the Spooler service (nwspool.dll) in Novell Client 4.91 SP2 through SP4 for Windows allow remote attackers to execute arbitrary code via certain long arguments to the (1) RpcAddPrinterDriver, (2) RpcGetPrinterDriverDirectory, and other unspecified RPC requests, aka Novell bug 300870, a different vulnerability than CVE-2006-5854.  
  
[CVE-2007-2966] Buffer overflow in the LHA decompression component in F-Secure anti-virus products for Microsoft Windows and Linux before 20070529 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted LHA archive, related to an integer wrap, a similar issue to CVE-2006-4335.  
  
[CVE-2007-2967] Multiple F-Secure anti-virus products for Microsoft Windows and Linux before 20070522 allow remote attackers to cause a denial of service (file scanning infinite loop) via certain crafted (1) ARJ archives or (2) FSG packed files.  
  
[CVE-2007-2999] Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.  
  
[CVE-2007-3028] "The LDAP service in Windows Active Directory in Microsoft Windows 2000 Server SP4 does not properly check ""the number of convertible attributes"", which allows remote attackers to cause a denial of service (service unavailability) via a crafted LDAP request, related to ""client sent LDAP request logic,"" aka ""Windows Active Directory Denial of Service Vulnerability"". NOTE: this is probably a different issue than CVE-2007-0040."  
  
[CVE-2007-3034] Integer overflow in the AttemptWrite function in Graphics Rendering Engine (GDI) on Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted metafile (image) with a large record length value, which triggers a heap-based buffer overflow.  
  
[CVE-2007-3035] "Unspecified vulnerability in Microsoft Windows Media Player 7.1, 9, 10, and 11 allows remote attackers to execute arbitrary code via a skin file (WMZ or WMD) with crafted header information that is not properly handled during decompression, aka ""Windows Media Player Code Execution Vulnerability Decompressing Skins."""  
  
[CVE-2007-3036] "Unspecified vulnerability in the (1) Windows Services for UNIX 3.0 and 3.5, and (2) Subsystem for UNIX-based Applications in Microsoft Windows 2000, XP, Server 2003, and Vista allows local users to gain privileges via unspecified vectors related to ""certain setuid binary files."""  
  
[CVE-2007-3037] "Microsoft Windows Media Player 7.1, 9, 10, and 11 allows remote attackers to execute arbitrary code via a skin file (WMZ or WMD) with crafted header information that causes a size mismatch between compressed and decompressed data and triggers a heap-based buffer overflow, aka ""Windows Media Player Code Execution Vulnerability Parsing Skins."""  
  
[CVE-2007-3038] "The Teredo interface in Microsoft Windows Vista and Vista x64 Edition does not properly handle certain network traffic, which allows remote attackers to bypass firewall blocking rules and obtain sensitive information via crafted IPv6 traffic, aka ""Windows Vista Firewall Blocking Rule Information Disclosure Vulnerability."""  
  
[CVE-2007-3040] Stack-based buffer overflow in agentdpv.dll 2.0.0.3425 in Microsoft Agent on Windows 2000 SP4 allows remote attackers to execute arbitrary code via a crafted URL to the Agent (Agent.Control) ActiveX control, which triggers an overflow within the Agent Service (agentsrv.exe) process, a different issue than CVE-2007-1205.  
  
[CVE-2007-3300] Multiple F-Secure anti-virus products for Microsoft Windows and Linux before 20070619 allow remote attackers to bypass scanning via a crafted header in a (1) LHA or (2) RAR archive.  
  
[CVE-2007-3406] "Multiple absolute path traversal vulnerabilities in Microsoft Internet Explorer 6 on Windows XP SP2 allow remote attackers to access arbitrary local files via the file: URI in the (1) src attribute of a (a) bgsound, (b) input, (c) EMBED, (d) img, or (e) script tag  
[CVE-2007-3436] Microsoft MSN Messenger 4.7 on Windows XP allows remote attackers to cause a denial of service (resource consumption) via a flood of SIP INVITE requests to the port specified for voice conversation.  
  
[CVE-2007-3463] "\*\* DISPUTED \*\* Microsoft Windows XP SP2 allows local users, who have sessions created by another user's RunAs (run as) command, to kill arbitrary processes of this other user, as demonstrated by the taskkill program. NOTE: the researcher claims a vendor dispute in which the vendor states that ""RunAs and UAC are convenience features, not security boundaries. If you need a security guarantee, please log out and log back in with a different account."""  
  
[CVE-2007-3509] Heap-based buffer overflow in the RPC subsystem in Symantec Backup Exec for Windows Servers 10.0, 10d, and 11d allows remote attackers to cause a denial of service (process exit) and possibly execute arbitrary code via crafted ncacn\_ip\_tcp requests.  
  
[CVE-2007-3671] "Unspecified vulnerability in the kernel in Microsoft Windows Vista has unspecified remote attack vectors and impact, as shown in the ""0day IPO"" presentation at SyScan'07."  
  
[CVE-2007-3724] "The process scheduler in the Microsoft Windows XP kernel does not make use of the process statistics kept by the kernel, performs scheduling based on CPU billing gathered from periodic process sampling ticks, and gives preference to ""interactive"" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in ""Secretly Monopolizing the CPU Without Superuser Privileges."""  
  
[CVE-2007-3826] Microsoft Internet Explorer 7 on Windows XP SP2 allows remote attackers to prevent users from leaving a site, spoof the address bar, and conduct phishing and other attacks via repeated document.open function calls after a user requests a new page, but before the onBeforeUnload function is called.  
  
[CVE-2007-3896] "The URL handling in Shell32.dll in the Windows shell in Microsoft Windows XP and Server 2003, with Internet Explorer 7 installed, allows remote attackers to execute arbitrary programs via invalid ""%"" sequences in a mailto: or other URI handler, as demonstrated using mIRC, Outlook, Firefox, Adobe Reader, Skype, and other applications. NOTE: this issue might be related to other issues involving URL handlers in Windows systems, such as CVE-2007-3845. There also might be separate but closely related issues in the applications that are invoked by the handlers."  
  
[CVE-2007-3897] Heap-based buffer overflow in Microsoft Outlook Express 6 and earlier, and Windows Mail for Vista, allows remote Network News Transfer Protocol (NNTP) servers to execute arbitrary code via long NNTP responses that trigger memory corruption.  
  
[CVE-2007-3898] The DNS server in Microsoft Windows 2000 Server SP4, and Server 2003 SP1 and SP2, uses predictable transaction IDs when querying other DNS servers, which allows remote attackers to spoof DNS replies, poison the DNS cache, and facilitate further attack vectors.  
  
[CVE-2007-3958] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service via a certain GIF file, as demonstrated by Art.gif.  
  
[CVE-2007-4218] "Multiple buffer overflows in the ServerProtect service (SpntSvc.exe) in Trend Micro ServerProtect for Windows before 5.58 Security Patch 4 allow remote attackers to execute arbitrary code via certain RPC requests to certain TCP ports that are processed by the (1) RPCFN\_ENG\_NewManualScan, (2) RPCFN\_ENG\_TimedNewManualScan, and (3) RPCFN\_SetComputerName functions in (a) StRpcSrv.dll  
[CVE-2007-4219] Integer overflow in the RPCFN\_SYNC\_TASK function in StRpcSrv.dll, as used by the ServerProtect service (SpntSvc.exe), in Trend Micro ServerProtect for Windows before 5.58 Security Patch 4 allows remote attackers to execute arbitrary code via a certain integer field in a request packet to TCP port 5168, which triggers a heap-based buffer overflow.  
  
[CVE-2007-4227] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service via a certain JPG file, as demonstrated by something.jpg. NOTE: this issue might be related to CVE-2007-3958.  
  
[CVE-2007-4247] Windows Calendar on Microsoft Windows Vista allows remote attackers to cause a denial of service (NULL dereference and persistent application crash) via a malformed ICS file.  
  
[CVE-2007-4288] Microsoft Windows Media Player 11 (wmplayer.exe) allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted .au file that triggers a divide-by-zero error, as demonstrated by iapetus.au.  
  
[CVE-2007-4414] "Cisco VPN Client on Windows before 4.8.02.0010 allows local users to gain privileges by enabling the ""Start Before Logon"" (SBL) and Microsoft Dial-Up Networking options, and then interacting with the dial-up networking dialog box."  
  
[CVE-2007-4490] Multiple buffer overflows in EarthAgent.exe in Trend Micro ServerProtect 5.58 for Windows before Security Patch 4 allow remote attackers to have an unknown impact via certain RPC function calls to (1) RPCFN\_EVENTBACK\_DoHotFix or (2) CMD\_CHANGE\_AGENT\_REGISTER\_INFO.  
  
[CVE-2007-5095] Microsoft Windows Media Player (WMP) 9 on Windows XP SP2 invokes Internet Explorer to render HTML documents contained inside some media files, regardless of what default web browser is configured, which might allow remote attackers to exploit vulnerabilities in software that the user does not expect to run, as demonstrated by the HTMLView parameter in an .asx file.  
  
[CVE-2007-5133] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service (CPU consumption) via a certain PNG file with a large tEXt chunk that possibly triggers an integer overflow in PNG chunk size handling, as demonstrated by badlycrafted.png.  
  
[CVE-2007-5145] Multiple buffer overflows in system DLL files in Microsoft Windows XP, as used by Microsoft Windows Explorer (explorer.exe) 6.00.2900.2180, Don Ho Notepad++, unspecified Adobe Macromedia applications, and other programs, allow user-assisted remote attackers to cause a denial of service (application crash) via long strings in the (1) author, (2) title, (3) subject, and (4) comment Properties fields of a file, possibly involving improper handling of extended file attributes by the (a) NtQueryInformationFile, (b) NtQueryDirectoryFile, (c) NtSetInformationFile, (d) FileAllInformation, (e) FileNameInformation, and other FILE\_INFORMATION\_CLASS functions in ntdll.dll and the (f) GetFileAttributesExW and (g) GetFileAttributesW functions in kernel32.dll, a related issue to CVE-2007-1347.  
  
[CVE-2007-5348] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via an image file with crafted gradient sizes in gradient fill input, which triggers a heap-based buffer overflow related to GdiPlus.dll and VGX.DLL, aka ""GDI+ VML Buffer Overrun Vulnerability."""  
  
[CVE-2007-5350] "Unspecified vulnerability in the Windows Advanced Local Procedure Call (ALPC) in the kernel in Microsoft Windows Vista allows local users to gain privileges via unspecified vectors involving ""legacy reply paths."""  
  
[CVE-2007-5351] "Unspecified vulnerability in Server Message Block Version 2 (SMBv2) signing support in Microsoft Windows Vista allows remote attackers to force signature re-computation and execute arbitrary code via a crafted SMBv2 packet, aka ""SMBv2 Signing Vulnerability."""  
  
[CVE-2007-5352] Unspecified vulnerability in Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2 allows local users to gain privileges via a crafted local procedure call (LPC) request.  
  
[CVE-2007-5460] Microsoft ActiveSync 4.1, as used in Windows Mobile 5.0, uses weak encryption (XOR obfuscation with a fixed key) when sending the user's PIN/Password over the USB connection from the host to the device, which might make it easier for attackers to decode a PIN/Password obtained by (1) sniffing or (2) spoofing the docking process.  
  
[CVE-2007-5587] Buffer overflow in Macrovision SafeDisc secdrv.sys before 4.3.86.0, as shipped in Microsoft Windows XP SP2, XP Professional x64 and x64 SP2, Server 2003 SP1 and SP2, and Server 2003 x64 and x64 SP2 allows local users to overwrite arbitrary memory locations and gain privileges via a crafted argument to a METHOD\_NEITHER IOCTL, as originally discovered in the wild.  
  
[CVE-2007-5633] Speedfan.sys in Alfredo Milani Comparetti SpeedFan 4.33, when used on Microsoft Windows Vista x64, allows local users to read or write arbitrary MSRs, and gain privileges and load unsigned drivers, via the (1) IOCTL\_RDMSR 0x9C402438 and (2) IOCTL\_WRMSR 0x9C40243C IOCTLs to \Device\speedfan, as demonstrated by an IOCTL\_WRMSR action on MSR\_LSTAR.  
  
[CVE-2007-5634] Speedfan.sys in Alfredo Milani Comparetti SpeedFan 4.33, when used on Microsoft Windows Vista x64, does not properly check a buffer during an IOCTL 0x9c402420 call, which allows local users to cause a denial of service (machine crash) and possibly gain privileges via unspecified vectors.  
  
[CVE-2007-6043] The CryptGenRandom function in Microsoft Windows 2000 generates predictable values, which makes it easier for context-dependent attackers to reduce the effectiveness of cryptographic mechanisms, as demonstrated by attacks on (1) forward security and (2) backward security, related to use of eight instances of the RC4 cipher, and possibly a related issue to CVE-2007-3898.  
  
[CVE-2007-6236] Microsoft Windows Media Player (WMP) allows remote attackers to cause a denial of service (application crash) via a certain AIFF file that triggers a divide-by-zero error, as demonstrated by kr.aiff.  
  
[CVE-2007-6332] The HPInfoDLL.HPInfo.1 ActiveX control in HPInfoDLL.dll 1.0, as shipped with HP Info Center (hpinfocenter.exe) 1.0.1.1 in HP Quick Launch Button (QLBCTRL.exe, aka QLB) 6.3 and earlier, on Microsoft Windows before Vista allows remote attackers to create or modify arbitrary registry values via the arguments to the SetRegValue method.  
  
[CVE-2007-6401] Stack-based buffer overflow in mplayer2.exe in Microsoft Windows Media Player (WMP) 6.4, when used with the 3ivx 4.5.1 or 5.0.1 codec, allows remote attackers to execute arbitrary code via a certain .mp4 file, possibly a related issue to CVE-2007-6402.  
  
[CVE-2007-6507] "SpntSvc.exe daemon in Trend Micro ServerProtect 5.58 for Windows, before Security Patch 4, exposes unspecified dangerous sub-functions from StRpcSrv.dll in the DCE/RPC interface, which allows remote attackers to obtain ""full file system access"" and execute arbitrary code."  
  
[CVE-2007-6701] Multiple stack-based buffer overflows in the Spooler service (nwspool.dll) in Novell Client 4.91 SP4 for Windows allow remote attackers to execute arbitrary code via long arguments to multiple unspecified RPC functions, aka Novell bug 287919, a different vulnerability than CVE-2007-2954.  
  
[CVE-2007-6753] Untrusted search path vulnerability in Shell32.dll in Microsoft Windows 2000, Windows XP, Windows Vista, Windows Server 2008, and Windows 7, when using an environment configured with a string such as %APPDATA% or %PROGRAMFILES% in a certain way, allows local users to gain privileges via a Trojan horse DLL under the current working directory, as demonstrated by iTunes and Safari.  
  
[CVE-2008-0015] "Stack-based buffer overflow in the CComVariant::ReadFromStream function in the Active Template Library (ATL), as used in the MPEG2TuneRequest ActiveX control in msvidctl.dll in DirectShow, in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted web page, as exploited in the wild in July 2009, aka ""Microsoft Video ActiveX Control Vulnerability."""  
  
[CVE-2008-0020] "Unspecified vulnerability in the Load method in the IPersistStreamInit interface in the Active Template Library (ATL), as used in the Microsoft Video ActiveX control in msvidctl.dll in DirectShow, in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via unknown vectors that trigger memory corruption, aka ""ATL Header Memcopy Vulnerability,"" a different vulnerability than CVE-2008-0015."  
  
[CVE-2008-0080] Heap-based buffer overflow in the WebDAV Mini-Redirector in Microsoft Windows XP SP2, Server 2003 SP1 and SP2, and Vista allows remote attackers to execute arbitrary code via a crafted WebDAV response.  
  
[CVE-2008-0083] The (1) VBScript (VBScript.dll) and (2) JScript (JScript.dll) scripting engines 5.1 and 5.6, as used in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2, do not properly decode script, which allows remote attackers to execute arbitrary code via unknown vectors.  
  
[CVE-2008-0084] Unspecified vulnerability in the TCP/IP support in Microsoft Windows Vista allows remote DHCP servers to cause a denial of service (hang and restart) via a crafted DHCP packet.  
  
[CVE-2008-0087] The DNS client in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, and Vista uses predictable DNS transaction IDs, which allows remote attackers to spoof DNS responses.  
  
[CVE-2008-0088] Unspecified vulnerability in Active Directory on Microsoft Windows 2000 and Windows Server 2003, and Active Directory Application Mode (ADAM) on XP and Server 2003, allows remote attackers to cause a denial of service (hang and restart) via a crafted LDAP request.  
  
[CVE-2008-0322] "The I2O Utility Filter driver (i2omgmt.sys) 5.1.2600.2180 for Microsoft Windows XP sets Everyone/Write permissions for the ""\\.\I2OExc"" device interface, which allows local users to gain privileges. NOTE: this issue can be leveraged to overwrite arbitrary memory and execute code via an IOCTL call with a crafted DeviceObject pointer."  
  
[CVE-2008-0639] Stack-based buffer overflow in the EnumPrinters function in the Spooler service (nwspool.dll) in Novell Client 4.91 SP2, SP3, and SP4 for Windows allows remote attackers to execute arbitrary code via a crafted RPC request, aka Novell bug 353138, a different vulnerability than CVE-2006-5854. NOTE: this issue exists because of an incomplete fix for CVE-2007-6701.  
  
[CVE-2008-0768] Multiple stack-based and heap-based buffer overflows in the Windows RPC components for IBM Informix Storage Manager (ISM), as used in Informix Dynamic Server (IDS) 10.00.xC8 and earlier and 11.10.xC2 and earlier, allow attackers to execute arbitrary code via crafted XDR requests.  
  
[CVE-2008-0951] Microsoft Windows Vista does not properly enforce the NoDriveTypeAutoRun registry value, which allows user-assisted remote attackers, and possibly physically proximate attackers, to execute arbitrary code by inserting a (1) CD-ROM device or (2) U3-enabled USB device containing a filesystem with an Autorun.inf file, and possibly other vectors related to (a) AutoRun and (b) AutoPlay actions.  
  
[CVE-2008-1083] "Heap-based buffer overflow in the CreateDIBPatternBrushPt function in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF or WMF image file with a malformed header that triggers an integer overflow, aka ""GDI Heap Overflow Vulnerability."""  
  
[CVE-2008-1084] Unspecified vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, through Vista SP1, and Server 2008 allows local users to execute arbitrary code via unknown vectors related to improper input validation. NOTE: it was later reported that one affected function is NtUserFnOUTSTRING in win32k.sys.  
  
[CVE-2008-1086] The HxTocCtrl ActiveX control (hxvz.dll), as used in Microsoft Internet Explorer 5.01 SP4 and 6 SP1, in Windows XP SP2, Server 2003 SP1 and SP2, Vista SP1, and Server 2008, allows remote attackers to execute arbitrary code via malformed arguments, which triggers memory corruption.  
  
[CVE-2008-1087] "Stack-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF image file with crafted filename parameters, aka ""GDI Stack Overflow Vulnerability."""  
  
[CVE-2008-1435] "Windows Explorer in Microsoft Windows Vista up to SP1, and Server 2008, allows user-assisted remote attackers to execute arbitrary code via crafted saved-search (.search-ms) files that are not properly handled when saving, aka ""Windows Saved Search Vulnerability."""  
  
[CVE-2008-1436] Microsoft Windows XP Professional SP2, Vista, and Server 2003 and 2008 does not properly assign activities to the (1) NetworkService and (2) LocalService accounts, which might allow context-dependent attackers to gain privileges by using one service process to capture a resource from a second service process that has a LocalSystem privilege-escalation ability, related to improper management of the SeImpersonatePrivilege user right, as originally reported for Internet Information Services (IIS), aka Token Kidnapping.  
  
[CVE-2008-1440] "Microsoft Windows XP SP2 and SP3, and Server 2003 SP1 and SP2, does not properly validate the option length field in Pragmatic General Multicast (PGM) packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted PGM packet, aka the ""PGM Invalid Length Vulnerability."""  
  
[CVE-2008-1441] "Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system hang) via a series of Pragmatic General Multicast (PGM) packets with invalid fragment options, aka the ""PGM Malformed Fragment Vulnerability."""  
  
[CVE-2008-1444] "Stack-based buffer overflow in Microsoft DirectX 7.0 and 8.1 on Windows 2000 SP4 allows remote attackers to execute arbitrary code via a Synchronized Accessible Media Interchange (SAMI) file with crafted parameters for a Class Name variable, aka the ""SAMI Format Parsing Vulnerability."""  
  
[CVE-2008-1445] Active Directory on Microsoft Windows 2000 Server SP4, XP Professional SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to cause a denial of service (system hang or reboot) via a crafted LDAP request.  
  
[CVE-2008-1446] "Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka ""Integer Overflow in IPP Service Vulnerability."""  
  
[CVE-2008-1448] "The MHTML protocol handler in a component of Microsoft Outlook Express 5.5 SP2 and 6 through SP1, and Windows Mail, does not assign the correct Internet Explorer Security Zone to UNC share pathnames, which allows remote attackers to bypass intended access restrictions and read arbitrary files via an mhtml: URI in conjunction with a redirection, aka ""URL Parsing Cross-Domain Information Disclosure Vulnerability."""  
  
[CVE-2008-1451] "The WINS service on Microsoft Windows 2000 SP4, and Server 2003 SP1 and SP2, does not properly validate data structures in WINS network packets, which allows local users to gain privileges via a crafted packet, aka ""Memory Overwrite Vulnerability."""  
  
[CVE-2008-1453] The Bluetooth stack in Microsoft Windows XP SP2 and SP3, and Vista Gold and SP1, allows physically proximate attackers to execute arbitrary code via a large series of Service Discovery Protocol (SDP) packets.  
  
[CVE-2008-1454] "Unspecified vulnerability in Microsoft DNS in Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 allows remote attackers to conduct cache poisoning attacks via unknown vectors related to accepting ""records from a response that is outside the remote server's authority,"" aka ""DNS Cache Poisoning Vulnerability,"" a different vulnerability than CVE-2008-1447."  
  
[CVE-2008-1456] Array index vulnerability in the Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote authenticated users to execute arbitrary code via a crafted event subscription request that is used to access an array of function pointers.  
  
[CVE-2008-1457] The Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate per-user subscriptions, which allows remote authenticated users to execute arbitrary code via a crafted event subscription request.  
  
[CVE-2008-1888] Cross-site scripting (XSS) vulnerability in Microsoft Windows SharePoint Services 2.0 allows remote attackers to inject arbitrary web script or HTML via the Picture Source (aka picture object source) field in the Rich Text Editor.  
  
[CVE-2008-2160] Multiple unspecified vulnerabilities in the JPEG (GDI+) and GIF image processing in Microsoft Windows CE 5.0 allow remote attackers to execute arbitrary code via crafted (1) JPEG and (2) GIF images.  
  
[CVE-2008-2245] Heap-based buffer overflow in the InternalOpenColorProfile function in mscms.dll in Microsoft Windows Image Color Management System (MSCMS) in the Image Color Management (ICM) component on Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted image file.  
  
[CVE-2008-2246] Microsoft Windows Vista through SP1 and Server 2008 do not properly import the default IPsec policy from a Windows Server 2003 domain to a Windows Server 2008 domain, which prevents IPsec rules from being enforced and allows remote attackers to bypass intended access restrictions.  
  
[CVE-2008-2249] "Integer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a malformed header in a crafted WMF file, which triggers a buffer overflow, aka ""GDI Integer Overflow Vulnerability."""  
  
[CVE-2008-2250] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate window properties sent from a parent window to a child window during creation of a new window, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Window Creation Vulnerability."""  
  
[CVE-2008-2251] "Double free vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that makes system calls within multiple threads, aka ""Windows Kernel Unhandled Exception Vulnerability."" NOTE: according to Microsoft, this is not a duplicate of CVE-2008-4510."  
  
[CVE-2008-2252] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate parameters sent from user mode to the kernel, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability."""  
  
[CVE-2008-2253] "Unspecified vulnerability in Microsoft Windows Media Player 11 allows remote attackers to execute arbitrary code via a crafted audio-only file that is streamed from a Server-Side Playlist (SSPL) on Windows Media Server, aka ""Windows Media Player Sampling Rate Vulnerability."""  
  
[CVE-2008-2540] "Apple Safari on Mac OS X, and before 3.1.2 on Windows, does not prompt the user before downloading an object that has an unrecognized content type, which allows remote attackers to place malware into the (1) Desktop directory on Windows or (2) Downloads directory on Mac OS X, and subsequently allows remote attackers to execute arbitrary code on Windows by leveraging an untrusted search path vulnerability in (a) Internet Explorer 7 on Windows XP or (b) the SearchPath function in Windows XP, Vista, and Server 2003 and 2008, aka a ""Carpet Bomb"" and a ""Blended Threat Elevation of Privilege Vulnerability,"" a different issue than CVE-2008-1032. NOTE: Apple considers this a vulnerability only because the Microsoft products can load application libraries from the desktop and, as of 20080619, has not covered the issue in an advisory for Mac OS X."  
  
[CVE-2008-2547] Stack-based buffer overflow in msiexec.exe 3.1.4000.1823 and 4.5.6001.22159 in Microsoft Windows Installer allows context-dependent attackers to execute arbitrary code via a long GUID value for the /x (aka /uninstall) option. NOTE: this issue might cross privilege boundaries if msiexec.exe is reachable via components such as ActiveX controls, and might additionally require a separate vulnerability in the control.  
  
[CVE-2008-3008] "Stack-based buffer overflow in the WMEncProfileManager ActiveX control in wmex.dll in Microsoft Windows Media Encoder 9 Series allows remote attackers to execute arbitrary code via a long first argument to the GetDetailsString method, aka ""Windows Media Encoder Buffer Overrun Vulnerability."""  
  
[CVE-2008-3009] "Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1, 9, and 2008 do not properly use the Service Principal Name (SPN) identifier when validating replies to authentication requests, which allows remote servers to execute arbitrary code via vectors that employ NTLM credential reflection, aka ""SPN Vulnerability."""  
  
[CVE-2008-3010] "Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1 and 9 incorrectly associate ISATAP addresses with the Local Intranet zone, which allows remote servers to capture NTLM credentials, and execute arbitrary code through credential-reflection attacks, by sending an authentication request, aka ""ISATAP Vulnerability."""  
  
[CVE-2008-3012] "gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 does not properly perform memory allocation, which allows remote attackers to execute arbitrary code via a malformed EMF image file, aka ""GDI+ EMF Memory Corruption Vulnerability."""  
  
[CVE-2008-3013] "gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed GIF image file containing many extension markers for graphic control extensions and subsequent unknown labels, aka ""GDI+ GIF Parsing Vulnerability."""  
  
[CVE-2008-3014] "Buffer overflow in gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed WMF image file that triggers improper memory allocation, aka ""GDI+ WMF Buffer Overrun Vulnerability."""  
  
[CVE-2008-3068] Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate embedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtain reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Authority Information Access (AIA) extension.  
  
[CVE-2008-3464] "afd.sys in the Ancillary Function Driver (AFD) component in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP1 and SP2 does not properly validate input sent from user mode to the kernel, which allows local users to gain privileges via a crafted application, as demonstrated using crafted pointers and lengths that bypass intended ProbeForRead and ProbeForWrite restrictions, aka ""AFD Kernel Overwrite Vulnerability."""  
  
[CVE-2008-3465] "Heap-based buffer overflow in an API in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows context-dependent attackers to cause a denial of service or execute arbitrary code via a WMF file with a malformed file-size parameter, which would not be properly handled by a third-party application that uses this API for a copy operation, aka ""GDI Heap Overflow Vulnerability."""  
  
[CVE-2008-3466] "Microsoft Host Integration Server (HIS) 2000, 2004, and 2006 does not limit RPC access to administrative functions, which allows remote attackers to bypass authentication and execute arbitrary programs via a crafted SNA RPC message using opcode 1 or 6 to call the CreateProcess function, aka ""HIS Command Execution Vulnerability."""  
  
[CVE-2008-3636] Integer overflow in the IopfCompleteRequest API in the kernel in Microsoft Windows 2000, XP, Server 2003, and Vista allows context-dependent attackers to gain privileges. NOTE: this issue was originally reported for GEARAspiWDM.sys 2.0.7.5 in Gear Software CD DVD Filter driver before 4.001.7, as used in other products including Apple iTunes and multiple Symantec and Norton products, which allows local users to gain privileges via repeated IoAttachDevice IOCTL calls to \\.\GEARAspiWDMDevice in this GEARAspiWDM.sys. However, the root cause is the integer overflow in the API call itself.  
  
[CVE-2008-3648] nslookup.exe in Microsoft Windows XP SP2 allows user-assisted remote attackers to execute arbitrary code, as demonstrated by an attempted DNS zone transfer, and as exploited in the wild in August 2008.  
  
[CVE-2008-3815] Unspecified vulnerability in Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)3, 7.1 before 7.1(2)78, 7.2 before 7.2(4)16, 8.0 before 8.0(4)6, and 8.1 before 8.1(1)13, when configured as a VPN using Microsoft Windows NT Domain authentication, allows remote attackers to bypass VPN authentication via unknown vectors.  
  
[CVE-2008-3893] Microsoft Bitlocker in Windows Vista before SP1 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer during boot, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.  
  
[CVE-2008-3957] "The Microsoft Windows Image Acquisition Logger ActiveX control allows remote attackers to force the download of arbitrary files onto a client system via a URL in the first argument to the Open method, in conjunction with a full destination pathname in the first argument to the Save method. NOTE: the provenance of this information is unknown  
[CVE-2008-4023] "Active Directory in Microsoft Windows 2000 SP4 does not properly allocate memory for (1) LDAP and (2) LDAPS requests, which allows remote attackers to execute arbitrary code via a crafted request, aka ""Active Directory Overflow Vulnerability."""  
  
[CVE-2008-4036] "Integer overflow in Memory Manager in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that triggers an erroneous decrement of a variable, related to validation of parameters for Virtual Address Descriptors (VADs) and a ""memory allocation mapping error,"" aka ""Virtual Address Descriptor Elevation of Privilege Vulnerability."""  
  
[CVE-2008-4037] "Microsoft Windows 2000 Gold through SP4, XP Gold through SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote SMB servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, as demonstrated by backrush, aka ""SMB Credential Reflection Vulnerability."" NOTE: some reliable sources report that this vulnerability exists because of an insufficient fix for CVE-2000-0834."  
  
[CVE-2008-4038] "Buffer underflow in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a Server Message Block (SMB) request that contains a filename with a crafted length, aka ""SMB Buffer Underflow Vulnerability."""  
  
[CVE-2008-4071] A certain ActiveX control in Adobe Acrobat 9, when used with Microsoft Windows Vista and Internet Explorer 7, allows remote attackers to cause a denial of service (browser crash) via an src property value with an invalid acroie:// URL.  
  
[CVE-2008-4127] Mshtml.dll in Microsoft Internet Explorer 7 Gold 7.0.5730 and 8 Beta 8.0.6001 on Windows XP SP2 allows remote attackers to cause a denial of service (failure of subsequent image rendering) via a crafted PNG file, related to an infinite loop in the CDwnTaskExec::ThreadExec function.  
  
[CVE-2008-4255] "Heap-based buffer overflow in mscomct2.ocx (aka Windows Common ActiveX control or Microsoft Animation ActiveX control) in Microsoft Visual Basic 6.0, Visual Studio .NET 2002 SP1 and 2003 SP1, Visual FoxPro 8.0 SP1 and 9.0 SP1 and SP2, and Office Project 2003 SP3 and 2007 Gold and SP1 allows remote attackers to execute arbitrary code via an AVI file with a crafted stream length, which triggers an ""allocation error"" and memory corruption, aka ""Windows Common AVI Parsing Overflow Vulnerability."""  
  
[CVE-2008-4261] "Stack-based buffer overflow in Microsoft Internet Explorer 5.01 SP4, 6 SP1 on Windows 2000, and 6 on Windows XP and Server 2003 does not properly handle extraneous data associated with an object embedded in a web page, which allows remote attackers to execute arbitrary code via crafted HTML tags that trigger memory corruption, aka ""HTML Rendering Memory Corruption Vulnerability."""  
  
[CVE-2008-4268] "The Windows Search component in Microsoft Windows Vista Gold and SP1 and Server 2008 does not properly free memory during a save operation for a Windows Search file, which allows remote attackers to execute arbitrary code via a crafted saved-search file, aka ""Windows Saved Search Vulnerability."""  
  
[CVE-2008-4269] "The search-ms protocol handler in Windows Explorer in Microsoft Windows Vista Gold and SP1 and Server 2008 uses untrusted parameter data obtained from incorrect parsing, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka ""Windows Search Parsing Vulnerability."""  
  
[CVE-2008-4295] Microsoft Windows Mobile 6.0 on HTC Wiza 200 and HTC MDA 8125 devices does not properly handle the first attempt to establish a Bluetooth connection to a peer with a long name, which allows remote attackers to cause a denial of service (device reboot) by configuring a Bluetooth device with a long hci name and (1) connecting directly to the Windows Mobile system or (2) waiting for the Windows Mobile system to scan for nearby devices.  
  
[CVE-2008-4323] Windows Explorer in Microsoft Windows XP SP3 allows user-assisted attackers to cause a denial of service (application crash) via a crafted .ZIP file.  
  
[CVE-2008-4327] gdiplus.dll in GDI+ in Microsoft Windows XP SP3 does not properly handle crafted .ico files, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a certain crash.ico file on a web site, and allows user-assisted attackers to cause a denial of service (divide-by-zero error and persistent application crash) via this crash.ico file on the desktop, a different vulnerability than CVE-2007-2237.  
  
[CVE-2008-4510] Microsoft Windows Vista Home and Ultimate Edition SP1 and earlier allows local users to cause a denial of service (page fault and system crash) via multiple attempts to access a virtual address in a PAGE\_NOACCESS memory page.  
  
[CVE-2008-4609] The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.  
  
[CVE-2008-4834] "Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via malformed values of unspecified ""fields inside the SMB packets"" in an NT Trans request, aka ""SMB Buffer Overflow Remote Code Execution Vulnerability."""  
  
[CVE-2008-4835] "SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via malformed values of unspecified ""fields inside the SMB packets"" in an NT Trans2 request, related to ""insufficiently validating the buffer size,"" aka ""SMB Validation Remote Code Execution Vulnerability."""  
  
[CVE-2008-4841] The WordPad Text Converter for Word 97 files in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted (1) .doc, (2) .wri, or (3) .rtf Word 97 file that triggers memory corruption, as exploited in the wild in December 2008. NOTE: As of 20081210, it is unclear whether this vulnerability is related to a WordPad issue disclosed on 20080925 with a 2008-crash.doc.rar example, but there are insufficient details to be sure.  
  
[CVE-2008-4927] "Microsoft Windows Media Player (WMP) 9.0 through 11 allows user-assisted attackers to cause a denial of service (application crash) via a malformed (1) MIDI or (2) DAT file, related to ""MThd Header Parsing."" NOTE: the provenance of this information is unknown  
[CVE-2008-5044] Race condition in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (crash or hang) via a multi-threaded application that makes many calls to UnhookWindowsHookEx while certain other desktop activity is occurring.  
  
[CVE-2008-5112] The LDAP server in Active Directory in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 responds differently to a failed bind attempt depending on whether the user account exists and is permitted to login, which allows remote attackers to enumerate valid usernames via a series of LDAP bind requests, as demonstrated by ldapuserenum.  
  
[CVE-2008-5179] Unspecified vulnerability in Microsoft Office Communications Server (OCS), Office Communicator, and Windows Live Messenger allows remote attackers to cause a denial of service (crash) via a crafted Real-time Transport Control Protocol (RTCP) receiver report packet.  
  
[CVE-2008-5229] "Stack-based buffer overflow in Microsoft Device IO Control in iphlpapi.dll in Microsoft Windows Vista Gold and SP1 allows local users in the Network Configuration Operator group to gain privileges or cause a denial of service (system crash) via a large invalid PrefixLength to the CreateIpForwardEntry2 method, as demonstrated by a ""route add"" command. NOTE: this issue might not cross privilege boundaries."  
  
[CVE-2008-5232] "Buffer overflow in the CallHTMLHelp method in the Microsoft Windows Media Services ActiveX control in nskey.dll 4.1.00.3917 in Windows Media Services on Microsoft Windows NT and 2000, and Avaya Media and Message Application servers, allows remote attackers to execute arbitrary code via a long argument. NOTE: the provenance of this information is unknown  
[CVE-2008-5415] The LDBserver service in the server in CA ARCserve Backup 11.1 through 12.0 on Windows allows remote attackers to execute arbitrary code via a handle\_t argument to an RPC endpoint in which the argument refers to an incompatible procedure.  
  
[CVE-2008-5745] Integer overflow in quartz.dll in the DirectShow framework in Microsoft Windows Media Player (WMP) 9, 10, and 11, including 11.0.5721.5260, allows remote attackers to cause a denial of service (application crash) via a crafted (1) WAV, (2) SND, or (3) MID file. NOTE: this has been incorrectly reported as a code-execution vulnerability. NOTE: it is not clear whether this issue is related to CVE-2008-4927.  
  
[CVE-2008-5750] Argument injection vulnerability in Microsoft Internet Explorer 8 beta 2 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI.  
  
[CVE-2008-5823] An ActiveX control in prtstb06.dll in Microsoft Money 2006, when used with WScript in Windows Script Host (WSH) on Windows Vista, allows remote attackers to cause a denial of service (access violation and application crash) via a zero value for the Startup property.  
  
[CVE-2008-5828] Microsoft Windows Live Messenger Client 8.5.1 and earlier, when MSN Protocol Version 15 (MSNP15) is used over a NAT session, allows remote attackers to discover intranet IP addresses and port numbers by reading the (1) IPv4InternalAddrsAndPorts, (2) IPv4Internal-Addrs, and (3) IPv4Internal-Port header fields.  
  
[CVE-2008-6194] Memory leak in the DNS server in Microsoft Windows allows remote attackers to cause a denial of service (memory consumption) via DNS packets. NOTE: this issue reportedly exists because of an incorrect fix for CVE-2007-3898.  
  
[CVE-2008-6219] nsrexecd.exe in multiple EMC Networker products including EMC NetWorker Server, Storage Node, and Client 7.3.x and 7.4, 7.4.1, 7.4.2, Client and Storage Node for Open VMS 7.3.2 ECO6 and earlier, Module for Microsoft Exchange 5.1 and earlier, Module for Microsoft Applications 2.0 and earlier, Module for Meditech 2.0 and earlier, and PowerSnap 2.4 SP1 and earlier does not properly control the allocation of memory, which allows remote attackers to cause a denial of service (memory exhaustion) via multiple crafted RPC requests.  
  
[CVE-2008-6819] win32k.sys in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (system crash) via vectors related to CreateWindow, TranslateMessage, and DispatchMessage, possibly a race condition between threads, a different vulnerability than CVE-2008-1084. NOTE: some of these details are obtained from third party information.  
  
[CVE-2009-0078] "The Windows Management Instrumentation (WMI) provider in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka ""Windows WMI Service Isolation Vulnerability."""  
  
[CVE-2009-0081] "The graphics device interface (GDI) implementation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate input received from user mode, which allows remote attackers to execute arbitrary code via a crafted (1) Windows Metafile (aka WMF) or (2) Enhanced Metafile (aka EMF) image file, aka ""Windows Kernel Input Validation Vulnerability."""  
  
[CVE-2009-0082] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate handles, which allows local users to gain privileges via a crafted application that triggers unspecified ""actions,"" aka ""Windows Kernel Handle Validation Vulnerability."""  
  
[CVE-2009-0083] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 does not properly handle invalid pointers, which allows local users to gain privileges via an application that triggers use of a crafted pointer, aka ""Windows Kernel Invalid Pointer Vulnerability."""  
  
[CVE-2009-0085] "The Secure Channel (aka SChannel) authentication component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008, when certificate authentication is used, does not properly validate the client's key exchange data in Transport Layer Security (TLS) handshake messages, which allows remote attackers to spoof authentication by crafting a TLS packet based on knowledge of the certificate but not the private key, aka ""SChannel Spoofing Vulnerability."""  
  
[CVE-2009-0086] "Integer underflow in Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote HTTP servers to execute arbitrary code via crafted parameter values in a response, related to error handling, aka ""Windows HTTP Services Integer Underflow Vulnerability."""  
  
[CVE-2009-0087] "Unspecified vulnerability in the Word 6 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2  
[CVE-2009-0089] "Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Vista Gold allows remote web servers to impersonate arbitrary https web sites by using DNS spoofing to ""forward a connection"" to a different https web site that has a valid certificate matching its own domain name, but not a certificate matching the domain name of the host requested by the user, aka ""Windows HTTP Services Certificate Name Mismatch Vulnerability."""  
  
[CVE-2009-0093] "Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not restrict registration of the ""wpad"" hostname, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) feature, and conduct man-in-the-middle attacks by spoofing a proxy server, via a Dynamic Update request for this hostname, aka ""DNS Server Vulnerability in WPAD Registration Vulnerability,"" a related issue to CVE-2007-1692."  
  
[CVE-2009-0094] "The WINS server in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 does not restrict registration of the (1) ""wpad"" and (2) ""isatap"" NetBIOS names, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) features, and conduct man-in-the-middle attacks by spoofing a proxy server or ISATAP route, by registering one of these names in the WINS database, aka ""WPAD WINS Server Registration Vulnerability,"" a related issue to CVE-2007-1692."  
  
[CVE-2009-0119] Buffer overflow in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .chm file.  
  
[CVE-2009-0202] "Array index error in FL21WIN.DLL in the PowerPoint Freelance Windows 2.1 Translator in Microsoft PowerPoint 2000 and 2002 allows remote attackers to execute arbitrary code via a Freelance file with unspecified ""layout information"" that triggers a heap-based buffer overflow."  
  
[CVE-2009-0229] "The Windows Printing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 allows local users to read arbitrary files via a crafted separator page, aka ""Print Spooler Read File Vulnerability."""  
  
[CVE-2009-0231] "The Embedded OpenType (EOT) Font Engine (T2EMBED.DLL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table in a data record that triggers an integer truncation and a heap-based buffer overflow, aka ""Embedded OpenType Font Heap Overflow Vulnerability."""  
  
[CVE-2009-0232] "Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table, aka ""Embedded OpenType Font Integer Overflow Vulnerability."""  
  
[CVE-2009-0233] "The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not reuse cached DNS responses in all applicable situations, which makes it easier for remote attackers to predict transaction IDs and poison caches by simultaneously sending crafted DNS queries and responses, aka ""DNS Server Query Validation Vulnerability."""  
  
[CVE-2009-0234] "The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 does not properly cache crafted DNS responses, which makes it easier for remote attackers to predict transaction IDs and poison caches by sending many crafted DNS queries that trigger ""unnecessary lookups,"" aka ""DNS Server Response Validation Vulnerability."""  
  
[CVE-2009-0235] "Stack-based buffer overflow in the Word 97 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted Word 97 file that triggers memory corruption, related to use of inconsistent integer data sizes for an unspecified length field, aka ""WordPad Word 97 Text Converter Stack Overflow Vulnerability."""  
  
[CVE-2009-0239] "Cross-site scripting (XSS) vulnerability in Windows Search 4.0 for Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows user-assisted remote attackers to inject arbitrary web script or HTML via a crafted file that appears in a preview in a search result, aka ""Script Execution in Windows Search Vulnerability."""  
  
[CVE-2009-0243] "Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutoRun registry values, which allows physically proximate attackers to execute arbitrary code by (1) inserting CD-ROM media, (2) inserting DVD media, (3) connecting a USB device, and (4) connecting a Firewire device  
[CVE-2009-0244] Directory traversal vulnerability in the OBEX FTP Service in the Microsoft Bluetooth stack in Windows Mobile 6 Professional, and probably Windows Mobile 5.0 for Pocket PC and 5.0 for Pocket PC Phone Edition, allows remote authenticated users to list arbitrary directories, and create or read arbitrary files, via a .. (dot dot) in a pathname. NOTE: this can be leveraged for code execution by writing to a Startup folder.  
  
[CVE-2009-0320] "Microsoft Windows XP, Server 2003 and 2008, and Vista exposes I/O activity measurements of all processes, which allows local users to obtain sensitive information, as demonstrated by reading the I/O Other Bytes column in Task Manager (aka taskmgr.exe) to estimate the number of characters that a different user entered at a runas.exe password prompt, related to a ""benchmarking attack."""  
  
[CVE-2009-0341] The shell32 module in Microsoft Internet Explorer 7.0 on Windows XP SP3 might allow remote attackers to execute arbitrary code via a long VALUE attribute in an INPUT element, possibly related to a stack consumption vulnerability.  
  
[CVE-2009-0550] "Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008  
[CVE-2009-0551] "Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 does not properly handle transition errors in a request for one HTTP document followed by a request for a second HTTP document, which allows remote attackers to execute arbitrary code via vectors involving (1) multiple crafted pages on a web site or (2) a web page with crafted inline content such as banner advertisements, aka ""Page Transition Memory Corruption Vulnerability."""  
  
[CVE-2009-0552] "Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 on Windows XP SP2 and SP3, and 6 on Windows Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0553] "Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0554] "Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0555] "Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly process Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted audio file that uses the Windows Media Speech codec, aka ""Windows Media Runtime Voice Sample Rate Vulnerability."""  
  
[CVE-2009-1043] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors triggered by clicking on a link, as demonstrated by Nils during a PWN2OWN competition at CanSecWest 2009.  
  
[CVE-2009-1122] "The WebDAV extension in Microsoft Internet Information Services (IIS) 5.0 on Windows 2000 SP4 does not properly decode URLs, which allows remote attackers to bypass authentication, and possibly read or create files, via a crafted HTTP request, aka ""IIS 5.0 WebDAV Authentication Bypass Vulnerability,"" a different vulnerability than CVE-2009-1535."  
  
[CVE-2009-1123] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate changes to unspecified kernel objects, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Desktop Vulnerability."""  
  
[CVE-2009-1124] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate user-mode pointers in unspecified error conditions, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Pointer Validation Vulnerability."""  
  
[CVE-2009-1125] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate an argument to an unspecified system call, which allows local users to gain privileges via a crafted application, aka ""Windows Driver Class Registration Vulnerability."""  
  
[CVE-2009-1126] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate the user-mode input associated with the editing of an unspecified desktop parameter, which allows local users to gain privileges via a crafted application, aka ""Windows Desktop Parameter Edit Vulnerability."""  
  
[CVE-2009-1127] "win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not correctly validate an argument to an unspecified system call, which allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka ""Win32k NULL Pointer Dereferencing Vulnerability."""  
  
[CVE-2009-1132] "Heap-based buffer overflow in the Wireless LAN AutoConfig Service (aka Wlansvc) in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed wireless frame, aka ""Wireless Frame Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2009-1133] "Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka ""Remote Desktop Connection Heap Overflow Vulnerability."""  
  
[CVE-2009-1138] "The LDAP service in Active Directory on Microsoft Windows 2000 SP4 does not properly free memory for LDAP and LDAPS requests, which allows remote attackers to execute arbitrary code via a request that uses hexadecimal encoding, whose associated memory is not released, related to a ""DN AttributeValue,"" aka ""Active Directory Invalid Free Vulnerability."" NOTE: this issue is probably a memory leak."  
  
[CVE-2009-1139] "Memory leak in the LDAP service in Active Directory on Microsoft Windows 2000 SP4 and Server 2003 SP2, and Active Directory Application Mode (ADAM) on Windows XP SP2 and SP3 and Server 2003 SP2, allows remote attackers to cause a denial of service (memory consumption and service outage) via (1) LDAP or (2) LDAPS requests with unspecified OID filters, aka ""Active Directory Memory Leak Vulnerability."""  
  
[CVE-2009-1141] "Microsoft Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via unspecified DHTML function calls related to a tr element and the ""insertion, deletion and attributes of a table cell,"" which trigger memory corruption when the window is destroyed, aka ""DHTML Object Memory Corruption Vulnerability."""  
  
[CVE-2009-1216] "Multiple unspecified vulnerabilities in (1) unlzh.c and (2) unpack.c in the gzip libraries in Microsoft Windows Server 2008, Windows Services for UNIX 3.0 and 3.5, and the Subsystem for UNIX-based Applications (SUA)  
[CVE-2009-1217] "Off-by-one error in the GpFont::SetData function in gdiplus.dll in Microsoft GDI+ on Windows XP allows remote attackers to cause a denial of service (stack corruption and application termination) via a crafted EMF file that triggers an integer overflow, as demonstrated by voltage-exploit.emf, aka the ""Microsoft GdiPlus EMF GpFont.SetData integer overflow."""  
  
[CVE-2009-1331] Integer overflow in Microsoft Windows Media Player (WMP) 11.0.5721.5260 allows remote attackers to cause a denial of service (application crash) via a crafted .mid file, as demonstrated by crash.mid.  
  
[CVE-2009-1335] Microsoft Internet Explorer 7 and 8 on Windows XP and Vista allows remote attackers to cause a denial of service (application hang) via a large document composed of unprintable characters, aka MSRC 9011jr.  
  
[CVE-2009-1511] GDI+ in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (infinite loop) via a PNG file that contains a certain large btChunkLen value.  
  
[CVE-2009-1528] "Microsoft Internet Explorer 6 and 7 for Windows XP SP2 and SP3  
[CVE-2009-1529] "Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1530] "Use-after-free vulnerability in Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1531] "Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1532] "Microsoft Internet Explorer 8 for Windows XP SP2 and SP3  
[CVE-2009-1533] "Buffer overflow in the Works for Windows document converters in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP3, Office 2007 SP1, and Works 8.5 and 9 allows remote attackers to execute arbitrary code via a crafted Works .wps file that triggers memory corruption, aka ""File Converter Buffer Overflow Vulnerability."""  
  
[CVE-2009-1537] "Unspecified vulnerability in the QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted QuickTime media file, as exploited in the wild in May 2009, aka ""DirectX NULL Byte Overwrite Vulnerability."""  
  
[CVE-2009-1538] "The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 performs updates to pointers without properly validating unspecified data values, which allows remote attackers to execute arbitrary code via a crafted QuickTime media file, aka ""DirectX Pointer Validation Vulnerability."""  
  
[CVE-2009-1539] "The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 does not properly validate unspecified size fields in QuickTime media files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""DirectX Size Validation Vulnerability."""  
  
[CVE-2009-1545] "Unspecified vulnerability in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed header in a crafted AVI file, aka ""Malformed AVI Header Vulnerability."""  
  
[CVE-2009-1546] "Integer overflow in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows allows remote attackers to execute arbitrary code on a Windows 2000 SP4 system via a crafted AVI file, or cause a denial of service on a Windows XP SP2 or SP3, Server 2003 SP2, Vista Gold, SP1, or SP2, or Server 2008 Gold or SP2 system via a crafted AVI file, aka ""AVI Integer Overflow Vulnerability."""  
  
[CVE-2009-1761] The message engine in CA ARCserve Backup r12.0 and r12.0 SP1 for Windows allows remote attackers to cause a denial of service (crash) via (1) an invalid 0x13 message, which is not properly handled in the ASCORE module, or (2) a 0x3B message with invalid stub data that triggers an RPC marshalling error.  
  
[CVE-2009-1808] Microsoft Windows XP SP3 allows local users to cause a denial of service (system crash) by making an SPI\_SETDESKWALLPAPER SystemParametersInfo call with an improperly terminated pvParam argument, followed by an SPI\_GETDESKWALLPAPER SystemParametersInfo call.  
  
[CVE-2009-1920] "The JScript scripting engine 5.1, 5.6, 5.7, and 5.8 in JScript.dll in Microsoft Windows, as used in Internet Explorer, does not properly load decoded scripts into memory before execution, which allows remote attackers to execute arbitrary code via a crafted web site that triggers memory corruption, aka ""JScript Remote Code Execution Vulnerability."""  
  
[CVE-2009-1922] "The Message Queuing (aka MSMQ) service for Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP2, and Vista Gold does not properly validate unspecified IOCTL request data from user mode before passing this data to kernel mode, which allows local users to gain privileges via a crafted request, aka ""MSMQ Null Pointer Vulnerability."""  
  
[CVE-2009-1923] "Heap-based buffer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted WINS replication packet that triggers an incorrect buffer-length calculation, aka ""WINS Heap Overflow Vulnerability."""  
  
[CVE-2009-1924] "Integer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 allows remote WINS replication partners to execute arbitrary code via crafted data structures in a packet, aka ""WINS Integer Overflow Vulnerability."""  
  
[CVE-2009-1925] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly manage state information, which allows remote attackers to execute arbitrary code by sending packets to a listening service, and thereby triggering misinterpretation of an unspecified field as a function pointer, aka ""TCP/IP Timestamps Code Execution Vulnerability."""  
  
[CVE-2009-1926] "Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to cause a denial of service (TCP outage) via a series of TCP sessions that have pending data and a (1) small or (2) zero receive window size, and remain in the FIN-WAIT-1 or FIN-WAIT-2 state indefinitely, aka ""TCP/IP Orphaned Connections Vulnerability."""  
  
[CVE-2009-1928] "Stack consumption vulnerability in the LDAP service in Active Directory on Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2  
[CVE-2009-1929] "Heap-based buffer overflow in the Microsoft Terminal Services Client ActiveX control running RDP 6.1 on Windows XP SP2, Vista SP1 or SP2, or Server 2008 Gold or SP2  
[CVE-2009-1930] "The Telnet service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote Telnet servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, aka ""Telnet Credential Reflection Vulnerability,"" a related issue to CVE-2000-0834."  
  
[CVE-2009-2357] The default configuration of TekRADIUS 3.0 uses the sa account to communicate with Microsoft SQL Server, which makes it easier for remote attackers to obtain privileged access to the database and the underlying Windows operating system.  
  
[CVE-2009-2484] Stack-based buffer overflow in the Win32AddConnection function in modules/access/smb.c in VideoLAN VLC media player 0.9.9, when running on Microsoft Windows, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long smb URI in a playlist file.  
  
[CVE-2009-2494] "The Active Template Library (ATL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via vectors related to erroneous free operations after reading a variant from a stream and deleting this variant, aka ""ATL Object Type Mismatch Vulnerability."""  
  
[CVE-2009-2498] "Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka ""Windows Media Header Parsing Invalid Free Vulnerability."""  
  
[CVE-2009-2499] "Microsoft Windows Media Format Runtime 9.0, 9.5, and 11  
[CVE-2009-2500] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted WMF image file, aka ""GDI+ WMF Integer Overflow Vulnerability."""  
  
[CVE-2009-2501] "Heap-based buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka ""GDI+ PNG Heap Overflow Vulnerability."""  
  
[CVE-2009-2502] "Buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted TIFF image file, aka ""GDI+ TIFF Buffer Overflow Vulnerability."""  
  
[CVE-2009-2503] "GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Windows Server 2003 SP2, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 does not properly allocate an unspecified buffer, which allows remote attackers to execute arbitrary code via a crafted TIFF image file that triggers memory corruption, aka ""GDI+ TIFF Memory Corruption Vulnerability."""  
  
[CVE-2009-2504] "Multiple integer overflows in unspecified APIs in GDI+ in Microsoft .NET Framework 1.1 SP1, .NET Framework 2.0 SP1 and SP2, Windows XP SP2 and SP3, Windows Server 2003 SP2, Vista Gold and SP1, Server 2008 Gold, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allow remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka ""GDI+ .NET API Vulnerability."""  
  
[CVE-2009-2505] "The Internet Authentication Service (IAS) in Microsoft Windows Vista SP2 and Server 2008 SP2 does not properly validate MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication requests, which allows remote attackers to execute arbitrary code via crafted structures in a malformed request, aka ""Internet Authentication Service Memory Corruption Vulnerability."""  
  
[CVE-2009-2507] "A certain ActiveX control in the Indexing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly process URLs, which allows remote attackers to execute arbitrary programs via unspecified vectors that cause a ""vulnerable binary"" to load and run, aka ""Memory Corruption in Indexing Service Vulnerability."""  
  
[CVE-2009-2508] "The single sign-on implementation in Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly remove credentials at the end of a network session, which allows physically proximate attackers to obtain the credentials of a previous user of the same web browser by using data from the browser's cache, aka ""Single Sign On Spoofing in ADFS Vulnerability."""  
  
[CVE-2009-2509] "Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly validate headers in HTTP requests, which allows remote authenticated users to execute arbitrary code via a crafted request to an IIS web server, aka ""Remote Code Execution in ADFS Vulnerability."""  
  
[CVE-2009-2510] "The CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, as used by Internet Explorer and other applications, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, aka ""Null Truncation in X.509 Common Name Vulnerability,"" a related issue to CVE-2009-2408."  
  
[CVE-2009-2511] "Integer overflow in the CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows man-in-the-middle attackers to spoof arbitrary SSL servers and other entities via an X.509 certificate that has a malformed ASN.1 Object Identifier (OID) and was issued by a legitimate Certification Authority, aka ""Integer Overflow in X.509 Object Identifiers Vulnerability."""  
  
[CVE-2009-2513] "The Graphics Device Interface (GDI) in win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Insufficient Data Validation Vulnerability."""  
  
[CVE-2009-2514] "win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not correctly parse font code during construction of a directory-entry table, which allows remote attackers to execute arbitrary code via a crafted Embedded OpenType (EOT) font, aka ""Win32k EOT Parsing Vulnerability."""  
  
[CVE-2009-2515] "Integer underflow in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows local users to gain privileges via a crafted application that triggers an incorrect truncation of a 64-bit integer to a 32-bit integer, aka ""Windows Kernel Integer Underflow Vulnerability."""  
  
[CVE-2009-2516] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly validate data sent from user mode, which allows local users to gain privileges via a crafted PE .exe file that triggers a NULL pointer dereference during chain traversal, aka ""Windows Kernel NULL Pointer Dereference Vulnerability."""  
  
[CVE-2009-2517] "The kernel in Microsoft Windows Server 2003 SP2 does not properly handle unspecified exceptions when an error condition occurs, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2009-2519] "The DHTML Editing Component ActiveX control in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly format HTML markup, which allows remote attackers to execute arbitrary code via a crafted web site that triggers ""system state"" corruption, aka ""DHTML Editing Component ActiveX Control Vulnerability."""  
  
[CVE-2009-2524] "Integer underflow in the NTLM authentication feature in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to cause a denial of service (reboot) via a malformed packet, aka ""Local Security Authority Subsystem Service Integer Overflow Vulnerability."""  
  
[CVE-2009-2525] "Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly initialize unspecified functions within compressed audio files, which allows remote attackers to execute arbitrary code via (1) a crafted media file or (2) crafted streaming content, aka ""Windows Media Runtime Heap Corruption Vulnerability."""  
  
[CVE-2009-2526] "Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 do not properly validate fields in SMBv2 packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted packet to the Server service, aka ""SMBv2 Infinite Loop Vulnerability."""  
  
[CVE-2009-2527] "Heap-based buffer overflow in Microsoft Windows Media Player 6.4 allows remote attackers to execute arbitrary code via (1) a crafted ASF file or (2) crafted streaming content, aka ""WMP Heap Overflow Vulnerability."""  
  
[CVE-2009-2532] "Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC do not properly process the command value in an SMB Multi-Protocol Negotiate Request packet, which allows remote attackers to execute arbitrary code via a crafted SMBv2 packet to the Server service, aka ""SMBv2 Command Value Vulnerability."""  
  
[CVE-2009-2544] Directory traversal vulnerability in the Marcelo Costa FileServer component 1.0 for Microsoft Windows Live Messenger and Messenger Plus! Live (MPL) allows remote authenticated users to list arbitrary directories and read arbitrary files via a .. (dot dot) in a pathname.  
  
[CVE-2009-2653] "\*\* DISPUTED \*\* The NtUserConsoleControl function in win32k.sys in Microsoft Windows XP SP2 and SP3, and Server 2003 before SP1, allows local administrators to bypass unspecified ""security software"" and gain privileges via a crafted call that triggers an overwrite of an arbitrary memory location. NOTE: the vendor disputes the significance of this report, stating that 'the Administrator to SYSTEM ""escalation"" is not a security boundary we defend.'"  
  
[CVE-2009-2655] mshtml.dll in Microsoft Internet Explorer 7 and 8 on Windows XP SP3 allows remote attackers to cause a denial of service (application crash) by calling the JavaScript findText method with a crafted Unicode string in the first argument, and only one additional argument, as demonstrated by a second argument of -1.  
  
[CVE-2009-2764] Microsoft Internet Explorer 8.0.7100.0 on Windows 7 RC on the x64 platform allows remote attackers to cause a denial of service (application crash) via a certain DIV element in conjunction with SCRIPT elements that have empty contents and no reference to a valid external script location.  
  
[CVE-2009-3019] Microsoft Internet Explorer 6 on Windows XP SP2 and SP3, and Internet Explorer 7 on Vista, allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls createElement to create an instance of the LI element, and then calls setAttribute to set the value attribute.  
  
[CVE-2009-3020] win32k.sys in Microsoft Windows Server 2003 SP2 allows remote attackers to cause a denial of service (system crash) by referencing a crafted .eot file in the src descriptor of an @font-face Cascading Style Sheets (CSS) rule in an HTML document, possibly related to the Embedded OpenType (EOT) Font Engine, a different vulnerability than CVE-2006-0010, CVE-2009-0231, and CVE-2009-0232. NOTE: some of these details are obtained from third party information.  
  
[CVE-2009-3103] "Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka ""SMBv2 Negotiation Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2009-3126] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka ""GDI+ PNG Integer Overflow Vulnerability."""  
  
[CVE-2009-3294] "The popen API function in TSRM/tsrm\_win32.c in PHP before 5.2.11 and 5.3.x before 5.3.1, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) ""e"" or (2) ""er"" string in the second argument (aka mode), possibly related to the \_fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function."  
  
[CVE-2009-3675] "LSASS.exe in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote authenticated users to cause a denial of service (CPU consumption) via a malformed ISAKMP request over IPsec, aka ""Local Security Authority Subsystem Service Resource Exhaustion Vulnerability."""  
  
[CVE-2009-3676] "The SMB client in the kernel in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to cause a denial of service (infinite loop and system hang) via a (1) SMBv1 or (2) SMBv2 response packet that contains (a) an incorrect length value in a NetBIOS header or (b) an additional length field at the end of this response packet, aka ""SMB Client Incomplete Response Vulnerability."""  
  
[CVE-2009-3677] "The Internet Authentication Service (IAS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly verify the credentials in an MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication request, which allows remote attackers to access network resources via a malformed request, aka ""MS-CHAP Authentication Bypass Vulnerability."""  
  
[CVE-2009-3678] "Integer overflow in cdd.dll in the Canonical Display Driver (CDD) in Microsoft Windows Server 2008 R2 and Windows 7 on 64-bit platforms, when the Windows Aero theme is installed, allows context-dependent attackers to cause a denial of service (reboot) or possibly execute arbitrary code via a crafted image file that triggers incorrect data parsing after user-mode data is copied to kernel mode, as demonstrated using ""Browse with Irfanview"" and certain actions on a folder containing a large number of thumbnail images in Resample mode, possibly related to the ATI graphics driver or win32k.sys, aka ""Canonical Display Driver Integer Overflow Vulnerability."""  
  
[CVE-2009-4210] The Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted media content.  
  
[CVE-2009-4309] Heap-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a large size value in a movi record in an IV41 stream in a media file, as demonstrated by an AVI file.  
  
[CVE-2009-4310] Stack-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted compressed video data in an IV41 stream in a media file, leading to many loop iterations, as demonstrated by data in an AVI file.  
  
[CVE-2009-4311] Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Paul Byrne of NGS Software. NOTE: this might overlap CVE-2008-3615.  
  
[CVE-2009-4312] Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Dave Lenoe of Adobe.  
  
[CVE-2009-4313] ir32\_32.dll 3.24.15.3 in the Indeo32 codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (heap corruption) or execute arbitrary code via malformed data in a stream in a media file, as demonstrated by an AVI file.  
  
[CVE-2010-0016] "The SMB client implementation in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate response fields, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted response, aka ""SMB Client Pool Corruption Vulnerability."""  
  
[CVE-2010-0017] "Race condition in the SMB client implementation in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code, and in the SMB client implementation in Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows local users to gain privileges, via a crafted SMB Negotiate response, aka ""SMB Client Race Condition Vulnerability."""  
  
[CVE-2010-0018] "Integer overflow in the Embedded OpenType (EOT) Font Engine (t2embed.dll) in Microsoft Windows 2000 SP4  
[CVE-2010-0019] "Microsoft Silverlight 3 before 3.0.50611.0 on Windows, and before 3.0.41130.0 on Mac OS X, does not properly handle pointers, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and framework outage) via a crafted web site, aka ""Microsoft Silverlight Memory Corruption Vulnerability."""  
  
[CVE-2010-0020] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate request fields, which allows remote authenticated users to execute arbitrary code via a malformed request, aka ""SMB Pathname Overflow Vulnerability."""  
  
[CVE-2010-0021] "Multiple race conditions in the SMB implementation in the Server service in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allow remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 Negotiate packet, aka ""SMB Memory Corruption Vulnerability."""  
  
[CVE-2010-0022] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate the share and servername fields in SMB packets, which allows remote attackers to cause a denial of service (system hang) via a crafted packet, aka ""SMB Null Pointer Vulnerability."""  
  
[CVE-2010-0023] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly kill processes after a logout, which allows local users to obtain sensitive information or gain privileges via a crafted application that continues to execute throughout the logout of one user and the login session of the next user, aka ""CSRSS Local Privilege Elevation Vulnerability."""  
  
[CVE-2010-0024] "The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2003 SP2, does not properly parse MX records, which allows remote DNS servers to cause a denial of service (service outage) via a crafted response to a DNS MX record query, aka ""SMTP Server MX Record Vulnerability."""  
  
[CVE-2010-0025] "The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2000 SP3, does not properly allocate memory for SMTP command replies, which allows remote attackers to read fragments of e-mail messages by sending a series of invalid commands and then sending a STARTTLS command, aka ""SMTP Memory Allocation Vulnerability."""  
  
[CVE-2010-0026] "The Hyper-V server implementation in Microsoft Windows Server 2008 Gold, SP2, and R2 on the x64 platform allows guest OS users to cause a denial of service (host OS hang) via a crafted application that executes a malformed series of machine instructions, aka ""Hyper-V Instruction Set Validation Vulnerability."""  
  
[CVE-2010-0027] "The URL validation functionality in Microsoft Internet Explorer 5.01, 6, 6 SP1, 7 and 8, and the ShellExecute API function in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, does not properly process input parameters, which allows remote attackers to execute arbitrary local programs via a crafted URL, aka ""URL Validation Vulnerability."""  
  
[CVE-2010-0028] "Integer overflow in Microsoft Paint in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted JPEG (.JPG) file, aka ""MS Paint Integer Overflow Vulnerability."""  
  
[CVE-2010-0035] "The Key Distribution Center (KDC) in Kerberos in Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2, when a trust relationship with a non-Windows Kerberos realm exists, allows remote authenticated users to cause a denial of service (NULL pointer dereference and domain controller outage) via a crafted Ticket Granting Ticket (TGT) renewal request, aka ""Kerberos Null Pointer Dereference Vulnerability."""  
  
[CVE-2010-0231] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not use a sufficient source of entropy, which allows remote attackers to obtain access to files and other SMB resources via a large number of authentication requests, related to server-generated challenges, certain ""duplicate values,"" and spoofing of an authentication token, aka ""SMB NTLM Authentication Lack of Entropy Vulnerability."""  
  
[CVE-2010-0232] "The kernel in Microsoft Windows NT 3.1 through Windows 7, including Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, when access to 16-bit applications is enabled on a 32-bit x86 platform, does not properly validate certain BIOS calls, which allows local users to gain privileges by crafting a VDM\_TIB data structure in the Thread Environment Block (TEB), and then calling the NtVdmControl function to start the Windows Virtual DOS Machine (aka NTVDM) subsystem, leading to improperly handled exceptions involving the #GP trap handler (nt!KiTrap0D), aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2010-0233] "Double free vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Double Free Vulnerability."""  
  
[CVE-2010-0234] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not properly validate a registry-key argument to an unspecified system call, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Null Pointer Vulnerability."""  
  
[CVE-2010-0235] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold does not perform the expected validation before creating a symbolic link, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Symbolic Link Value Vulnerability."""  
  
[CVE-2010-0236] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold does not properly allocate memory for the destination key associated with a symbolic-link registry key, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Allocation Vulnerability."""  
  
[CVE-2010-0237] "The kernel in Microsoft Windows 2000 SP4 and XP SP2 and SP3 allows local users to gain privileges by creating a symbolic link from an untrusted registry hive to a trusted registry hive, aka ""Windows Kernel Symbolic Link Creation Vulnerability."""  
  
[CVE-2010-0238] "Unspecified vulnerability in registry-key validation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Registry Key Vulnerability."""  
  
[CVE-2010-0239] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Router Advertisement packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""ICMPv6 Router Advertisement Vulnerability."""  
  
[CVE-2010-0240] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when a custom network driver is used, does not properly handle local fragmentation of Encapsulating Security Payload (ESP) over UDP packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""Header MDL Fragmentation Vulnerability."""  
  
[CVE-2010-0241] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Route Information packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""ICMPv6 Route Information Vulnerability."""  
  
[CVE-2010-0242] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to cause a denial of service (system hang) via crafted packets with malformed TCP selective acknowledgement (SACK) values, aka ""TCP/IP Selective Acknowledgement Vulnerability."""  
  
[CVE-2010-0249] "Use-after-free vulnerability in Microsoft Internet Explorer 6, 6 SP1, 7, and 8 on Windows 2000 SP4  
[CVE-2010-0250] "Heap-based buffer overflow in DirectShow in Microsoft DirectX, as used in the AVI Filter on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2, and in Quartz on Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, allows remote attackers to execute arbitrary code via an AVI file with a crafted length field in an unspecified video stream, which is not properly handled by the RLE video decompressor, aka ""DirectShow Heap Overflow Vulnerability."""  
  
[CVE-2010-0252] "The Microsoft Data Analyzer ActiveX control (aka the Office Excel ActiveX control for Data Analysis) in max3activex.dll in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to execute arbitrary code via a crafted web page that corrupts the ""system state,"" aka ""Microsoft Data Analyzer ActiveX Control Vulnerability."""  
  
[CVE-2010-0265] "Buffer overflow in Microsoft Windows Movie Maker 2.1, 2.6, and 6.0, and Microsoft Producer 2003, allows remote attackers to execute arbitrary code via a crafted project (.MSWMM) file, aka ""Movie Maker and Producer Buffer Overflow Vulnerability."""  
  
[CVE-2010-0268] "Unspecified vulnerability in the Windows Media Player ActiveX control in Windows Media Player (WMP) 9 on Microsoft Windows 2000 SP4 and XP SP2 and SP3 allows remote attackers to execute arbitrary code via crafted media content, aka ""Media Player Remote Code Execution Vulnerability."""  
  
[CVE-2010-0269] "The SMB client in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for SMB responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Memory Allocation Vulnerability."""  
  
[CVE-2010-0270] "The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate fields in SMB transaction responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Transaction Vulnerability."""  
  
[CVE-2010-0278] A certain ActiveX control in msgsc.14.0.8089.726.dll in Microsoft Windows Live Messenger 2009 build 14.0.8089.726 on Windows Vista and Windows 7 allows remote attackers to cause a denial of service (msnmsgr.exe crash) by calling the ViewProfile method with a crafted argument during an MSN Messenger session.  
  
[CVE-2010-0378] "Use-after-free vulnerability in Adobe Flash Player 6.0.79, as distributed in Microsoft Windows XP SP2 and SP3, allows remote attackers to execute arbitrary code by unloading a Flash object that is currently being accessed by a script, leading to memory corruption, aka a ""Movie Unloading Vulnerability."""  
  
[CVE-2010-0379] "Multiple unspecified vulnerabilities in the Macromedia Flash ActiveX control in Adobe Flash Player 6, as distributed in Microsoft Windows XP SP2 and SP3, might allow remote attackers to execute arbitrary code via unspecified vectors that are not related to the use-after-free ""Movie Unloading Vulnerability"" (CVE-2010-0378). NOTE: due to lack of details, it is not clear whether this overlaps any other CVE item."  
  
[CVE-2010-0476] "The SMB client in Microsoft Windows Server 2003 SP2, Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted SMB transaction response that uses (1) SMBv1 or (2) SMBv2, aka ""SMB Client Response Parsing Vulnerability."""  
  
[CVE-2010-0477] "The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly handle (1) SMBv1 and (2) SMBv2 response packets, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted packet that causes the client to read the entirety of the response, and then improperly interact with the Winsock Kernel (WSK), aka ""SMB Client Message Size Vulnerability."""  
  
[CVE-2010-0478] "Stack-based buffer overflow in nsum.exe in the Windows Media Unicast Service in Media Services for Microsoft Windows 2000 Server SP4 allows remote attackers to execute arbitrary code via crafted packets associated with transport information, aka ""Media Services Stack-based Buffer Overflow Vulnerability."""  
  
[CVE-2010-0480] "Multiple stack-based buffer overflows in the MPEG Layer-3 audio codecs in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to execute arbitrary code via a crafted AVI file, aka ""MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability."""  
  
[CVE-2010-0481] "The kernel in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly translate a registry key's virtual path to its real path, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Virtual Path Parsing Vulnerability."""  
  
[CVE-2010-0482] "The kernel in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate relocation sections of image files, which allows local users to cause a denial of service (reboot) via a crafted file, aka ""Windows Kernel Malformed Image Vulnerability."""  
  
[CVE-2010-0483] "vbscript.dll in VBScript 5.1, 5.6, 5.7, and 5.8 in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, allows user-assisted remote attackers to execute arbitrary code by referencing a (1) local pathname, (2) UNC share pathname, or (3) WebDAV server with a crafted .hlp file in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution involving winhlp32.exe when the F1 key is pressed, aka ""VBScript Help Keypress Vulnerability."""  
  
[CVE-2010-0484] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 ""do not properly validate changes in certain kernel objects,"" which allows local users to execute arbitrary code via vectors related to Device Contexts (DC) and the GetDCEx function, aka ""Win32k Improper Data Validation Vulnerability."""  
  
[CVE-2010-0485] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 Gold and SP2, Windows 7, and Server 2008 R2 ""do not properly validate all callback parameters when creating a new window,"" which allows local users to execute arbitrary code, aka ""Win32k Window Creation Vulnerability."""  
  
[CVE-2010-0486] "The WinVerifyTrust function in Authenticode Signature Verification 5.1, 6.0, and 6.1 in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly use unspecified fields in a file digest, which allows user-assisted remote attackers to execute arbitrary code via a modified (1) Portable Executable (PE) or (2) cabinet (aka .CAB) file that incorrectly appears to have a valid signature, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2010-0487] "The Authenticode Signature verification functionality in cabview.dll in Cabinet File Viewer Shell Extension 5.1, 6.0, and 6.1 in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly use unspecified fields in a file digest, which allows remote attackers to execute arbitrary code via a modified cabinet (aka .CAB) file that incorrectly appears to have a valid signature, aka ""Cabview Corruption Validation Vulnerability."""  
  
[CVE-2010-0718] Buffer overflow in Microsoft Windows Media Player 9 and 11.0.5721.5145 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted .mpg file.  
  
[CVE-2010-0719] An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.  
  
[CVE-2010-0805] "The Tabular Data Control (TDC) ActiveX control in Microsoft Internet Explorer 5.01 SP4, 6 on Windows XP SP2 and SP3, and 6 SP1 allows remote attackers to execute arbitrary code via a long URL (DataURL parameter) that triggers memory corruption in the CTDCCtl::SecurityCHeckDataURL function, aka ""Memory Corruption Vulnerability."""  
  
[CVE-2010-0808] "Microsoft Internet Explorer 6 and 7 on Windows XP and Vista does not prevent script from simulating user interaction with the AutoComplete feature, which allows remote attackers to obtain sensitive form information via a crafted web site, aka ""AutoComplete Information Disclosure Vulnerability."""  
  
[CVE-2010-0810] "The kernel in Microsoft Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, does not properly handle unspecified exceptions, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2010-0811] "Multiple unspecified vulnerabilities in the Microsoft Internet Explorer 8 Developer Tools ActiveX control in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow remote attackers to execute arbitrary code via unknown vectors that ""corrupt the system state,"" aka ""Microsoft Internet Explorer 8 Developer Tools Vulnerability."""  
  
[CVE-2010-0812] "Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to bypass intended IPv4 source-address restrictions via a mismatched IPv6 source address in a tunneled ISATAP packet, aka ""ISATAP IPv6 Source Address Spoofing Vulnerability."""  
  
[CVE-2010-0818] "The MPEG-4 codec in the Windows Media codecs in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly handle crafted media content with MPEG-4 video encoding, which allows remote attackers to execute arbitrary code via a file in an unspecified ""supported format,"" aka ""MPEG-4 Codec Vulnerability."""  
  
[CVE-2010-0819] "Unspecified vulnerability in the Windows OpenType Compact Font Format (CFF) driver in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users to execute arbitrary code via unknown vectors related to improper validation when copying data from user mode to kernel mode, aka ""OpenType CFF Font Driver Memory Corruption Vulnerability."""  
  
[CVE-2010-0820] "Heap-based buffer overflow in the Local Security Authority Subsystem Service (LSASS), as used in Active Directory in Microsoft Windows Server 2003 SP2 and Windows Server 2008 Gold, SP2, and R2  
[CVE-2010-0917] Stack-based buffer overflow in VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, might allow user-assisted remote attackers to execute arbitrary code via a long string in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution when the F1 key is pressed, a different vulnerability than CVE-2010-0483.  
  
[CVE-2010-1042] "Microsoft Windows Media Player 11 does not properly perform colorspace conversion, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted .AVI file. NOTE: the provenance of this information is unknown  
[CVE-2010-1098] The ANI parser in Microsoft Windows before 7 on the x86 platform, as used in Internet Explorer and other applications, allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted biClrUsed value in the BITMAPINFO header of a .ANI file.  
  
[CVE-2010-1117] Heap-based buffer overflow in Internet Explorer 8 on Microsoft Windows 7 allows remote attackers to discover the base address of a Windows .dll file, and possibly have unspecified other impact, via unknown vectors, as demonstrated by Peter Vreugdenhil during a Pwn2Own competition at CanSecWest 2010.  
  
[CVE-2010-1118] Unspecified vulnerability in Internet Explorer 8 on Microsoft Windows 7 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to a use-after-free issue, as demonstrated by Peter Vreugdenhil during a Pwn2Own competition at CanSecWest 2010.  
  
[CVE-2010-1175] "Microsoft Internet Explorer 7.0 on Windows XP and Windows Server 2003 allows remote attackers to have an unspecified impact via a certain XML document that references a crafted web site in the SRC attribute of an image element, related to a ""0day Vulnerability."""  
  
[CVE-2010-1225] "The memory-management implementation in the Virtual Machine Monitor (aka VMM or hypervisor) in Microsoft Virtual PC 2007 Gold and SP1, Virtual Server 2005 Gold and R2 SP1, and Windows Virtual PC does not properly restrict access from the guest OS to memory locations in the VMM work area, which allows context-dependent attackers to bypass certain anti-exploitation protection mechanisms on the guest OS via crafted input to a vulnerable application. NOTE: the vendor reportedly found that only systems with an otherwise vulnerable application are affected, because ""the memory areas accessible from the guest cannot be leveraged to achieve either remote code execution or elevation of privilege and ... no data from the host is exposed to the guest OS."""  
  
[CVE-2010-1255] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 Gold and SP2, Windows 7, and Server 2008 R2 allows local users to execute arbitrary code via vectors related to ""glyph outline information"" and TrueType fonts, aka ""Win32k TrueType Font Parsing Vulnerability."""  
  
[CVE-2010-1263] "Windows Shell and WordPad in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7  
[CVE-2010-1264] "Unspecified vulnerability in Microsoft Windows SharePoint Services 3.0 SP1 and SP2 allows remote attackers to cause a denial of service (hang) via crafted requests to the Help page that cause repeated restarts of the application pool, aka ""Sharepoint Help Page Denial of Service Vulnerability."""  
  
[CVE-2010-1689] The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 uses predictable transaction IDs that are formed by incrementing a previous ID by 1, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.  
  
[CVE-2010-1690] The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 does not verify that transaction IDs of responses match transaction IDs of queries, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.  
  
[CVE-2010-1734] The SfnINSTRING function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x18d value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.  
  
[CVE-2010-1735] The SfnLOGONNOTIFY function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x4c value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.  
  
[CVE-2010-1880] "Unspecified vulnerability in Quartz.dll for DirectShow on Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1, and Server 2008 allows remote attackers to execute arbitrary code via a media file with crafted compression data, aka ""MJPEG Media Decompression Vulnerability."""  
  
[CVE-2010-1882] "Multiple buffer overflows in the MPEG Layer-3 Audio Codec for Microsoft DirectShow in l3codecx.ax in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allow remote attackers to execute arbitrary code via an MPEG Layer-3 audio stream in (1) a crafted media file or (2) crafted streaming content, aka ""MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability."""  
  
[CVE-2010-1883] "Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to execute arbitrary code via a crafted table in an embedded font, aka ""Embedded OpenType Font Integer Overflow Vulnerability."""  
  
[CVE-2010-1885] "The MPC::HexToNum function in helpctr.exe in Microsoft Windows Help and Support Center in Windows XP and Windows Server 2003 does not properly handle malformed escape sequences, which allows remote attackers to bypass the trusted documents whitelist (fromHCP option) and execute arbitrary commands via a crafted hcp:// URL, aka ""Help Center URL Validation Vulnerability."""  
  
[CVE-2010-1886] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2, and Windows 7 allow local users to gain privileges by leveraging access to a process with NetworkService credentials, as demonstrated by TAPI Server, SQL Server, and IIS processes, and related to the Windows Service Isolation feature. NOTE: the vendor states that privilege escalation from NetworkService to LocalSystem does not cross a ""security boundary."""  
  
[CVE-2010-1887] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly validate an unspecified system-call argument, which allows local users to cause a denial of service (system hang) via a crafted application, aka ""Win32k Bounds Checking Vulnerability."""  
  
[CVE-2010-1888] "Race condition in the kernel in Microsoft Windows XP SP3 allows local users to gain privileges via vectors involving thread creation, aka ""Windows Kernel Data Initialization Vulnerability."""  
  
[CVE-2010-1889] "Double free vulnerability in the kernel in Microsoft Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2, allows local users to gain privileges via a crafted application, related to object initialization during error handling, aka ""Windows Kernel Double Free Vulnerability."""  
  
[CVE-2010-1890] "The kernel in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate ACLs on kernel objects, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Improper Validation Vulnerability."""  
  
[CVE-2010-1891] "The Client/Server Runtime Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2, when a Chinese, Japanese, or Korean locale is enabled, does not properly allocate memory for transactions, which allows local users to gain privileges via a crafted application, aka ""CSRSS Local Elevation of Privilege Vulnerability."""  
  
[CVE-2010-1892] "The TCP/IP stack in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly handle malformed IPv6 packets, which allows remote attackers to cause a denial of service (system hang) via multiple crafted packets, aka ""IPv6 Memory Corruption Vulnerability."""  
  
[CVE-2010-1893] "Integer overflow in the TCP/IP stack in Microsoft Windows Vista SP1, Windows Server 2008 Gold and R2, and Windows 7 allows local users to gain privileges via a buffer of user-mode data that is copied to kernel mode, aka ""Integer Overflow in Windows Networking Vulnerability."""  
  
[CVE-2010-1894] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, do not properly handle unspecified exceptions, which allows local users to gain privileges via a crafted application, aka ""Win32k Exception Handling Vulnerability."""  
  
[CVE-2010-1895] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, do not properly perform memory allocation before copying user-mode data to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Win32k Pool Overflow Vulnerability."""  
  
[CVE-2010-1896] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 do not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Win32k User Input Validation Vulnerability."""  
  
[CVE-2010-1897] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly validate pseudo-handle values in callback parameters during window creation, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Creation Vulnerability."""  
  
[CVE-2010-1898] "The Common Language Runtime (CLR) in Microsoft .NET Framework 2.0 SP1, 2.0 SP2, 3.5, 3.5 SP1, and 3.5.1, and Microsoft Silverlight 2 and 3 before 3.0.50611.0 on Windows and before 3.0.41130.0 on Mac OS X, does not properly handle interfaces and delegations to virtual methods, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (aka XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka ""Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability."""  
  
[CVE-2010-2091] Microsoft Outlook Web Access (OWA) 8.2.254.0, when Internet Explorer 7 on Windows Server 2003 is used, does not properly handle the id parameter in a Folder IPF.Note action to the default URI, which might allow remote attackers to obtain sensitive information or conduct cross-site scripting (XSS) attacks via an invalid value.  
  
[CVE-2010-2265] Cross-site scripting (XSS) vulnerability in the GetServerName function in sysinfo/commonFunc.js in Microsoft Windows Help and Support Center for Windows XP and Windows Server 2003 allows remote attackers to inject arbitrary web script or HTML via the svr parameter to sysinfo/sysinfomain.htm. NOTE: this can be leveraged with CVE-2010-1885 to execute arbitrary commands without user interaction.  
  
[CVE-2010-2549] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2 and Server 2008 Gold and SP2 allows local users to gain privileges or cause a denial of service (system crash) by using a large number of calls to the NtUserCheckAccessForIntegrityLevel function to trigger a failure in the LockProcessByClientId function, leading to deletion of an in-use process object, aka ""Win32k Reference Count Vulnerability."""  
  
[CVE-2010-2550] "The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate fields in an SMB request, which allows remote attackers to execute arbitrary code via a crafted SMB packet, aka ""SMB Pool Overflow Vulnerability."""  
  
[CVE-2010-2551] "The SMB Server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate an internal variable in an SMB packet, which allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 packet, aka ""SMB Variable Validation Vulnerability."""  
  
[CVE-2010-2552] "Stack consumption vulnerability in the SMB Server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to cause a denial of service (system hang) via a malformed SMBv2 compounded request, aka ""SMB Stack Exhaustion Vulnerability."""  
  
[CVE-2010-2553] "The Cinepak codec in Microsoft Windows XP SP2 and SP3, Windows Vista SP1 and SP2, and Windows 7 does not properly decompress media files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""Cinepak Codec Decompression Vulnerability."""  
  
[CVE-2010-2554] "The Tracing Feature for Services in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 has incorrect ACLs on its registry keys, which allows local users to gain privileges via vectors involving a named pipe and impersonation, aka ""Tracing Registry Key ACL Vulnerability."""  
  
[CVE-2010-2555] "The Tracing Feature for Services in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the length of strings in the registry, which allows local users to gain privileges or cause a denial of service (memory corruption) via vectors involving a long string, aka ""Tracing Memory Corruption Vulnerability."""  
  
[CVE-2010-2563] "The Word 97 text converter in the WordPad Text Converters in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly parse malformed structures in Word 97 documents, which allows remote attackers to execute arbitrary code via a crafted document containing an unspecified value that is used in a loop counter, aka ""WordPad Word 97 Text Converter Memory Corruption Vulnerability."""  
  
[CVE-2010-2564] "Buffer overflow in Microsoft Windows Movie Maker (WMM) 2.1, 2.6, and 6.0 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted project file, aka ""Movie Maker Memory Corruption Vulnerability."""  
  
[CVE-2010-2566] "The Secure Channel (aka SChannel) security package in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, does not properly validate certificate request messages from TLS and SSL servers, which allows remote servers to execute arbitrary code via a crafted SSL response, aka ""SChannel Malformed Certificate Request Remote Code Execution Vulnerability."""  
  
[CVE-2010-2568] Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.  
  
[CVE-2010-2731] "Unspecified vulnerability in Microsoft Internet Information Services (IIS) 5.1 on Windows XP SP3, when directory-based Basic Authentication is enabled, allows remote attackers to bypass intended access restrictions and execute ASP files via a crafted request, aka ""Directory Authentication Bypass Vulnerability."""  
  
[CVE-2010-2738] "The Uniscribe (aka new Unicode Script Processor) implementation in USP10.DLL in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2, and Microsoft Office XP SP3, 2003 SP3, and 2007 SP2, does not properly validate tables associated with malformed OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) Office document, aka ""Uniscribe Font Parsing Engine Memory Corruption Vulnerability."""  
  
[CVE-2010-2739] Buffer overflow in the CreateDIBPalette function in win32k.sys in Microsoft Windows XP SP3, Server 2003 R2 Enterprise SP2, Vista Business SP1, Windows 7, and Server 2008 SP2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.  
  
[CVE-2010-2740] "The OpenType Font (OTF) format driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly perform memory allocation during font parsing, which allows local users to gain privileges via a crafted application, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2010-2741] "The OpenType Font (OTF) format driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 performs an incorrect integer calculation during font processing, which allows local users to gain privileges via a crafted application, aka ""OpenType Font Validation Vulnerability."""  
  
[CVE-2010-2743] "The kernel-mode drivers in Microsoft Windows XP SP3 do not properly perform indexing of a function-pointer table during the loading of keyboard layouts from disk, which allows local users to gain privileges via a crafted application, as demonstrated in the wild in July 2010 by the Stuxnet worm, aka ""Win32k Keyboard Layout Vulnerability."" NOTE: this might be a duplicate of CVE-2010-3888 or CVE-2010-3889."  
  
[CVE-2010-2744] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly manage a window class, which allows local users to gain privileges by creating a window, then using (1) the SetWindowLongPtr function to modify the popup menu structure, or (2) the SwitchWndProc function with a switch window information pointer, which is not re-initialized when a WM\_NCCREATE message is processed, aka ""Win32k Window Class Vulnerability."""  
  
[CVE-2010-2745] "Microsoft Windows Media Player (WMP) 9 through 12 does not properly deallocate objects during a browser reload action, which allows user-assisted remote attackers to execute arbitrary code via crafted media content referenced in an HTML document, aka ""Windows Media Player Memory Corruption Vulnerability."""  
  
[CVE-2010-2746] "Heap-based buffer overflow in Comctl32.dll (aka the common control library) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when a third-party SVG viewer is used, allows remote attackers to execute arbitrary code via a crafted HTML document that triggers unspecified messages from this viewer, aka ""Comctl32 Heap Overflow Vulnerability."""  
  
[CVE-2010-3138] "Untrusted search path vulnerability in the Indeo Codec in iac25\_32.ax in Microsoft Windows XP SP3 allows local users to gain privileges via a Trojan horse iacenc.dll file in the current working directory, as demonstrated by access through BS.Player or Media Player Classic to a directory that contains a .avi, .mka, .ra, or .ram file, aka ""Indeo Codec Insecure Library Loading Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2010-3140] Untrusted search path vulnerability in Microsoft Windows Internet Communication Settings on Windows XP SP3 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse schannel.dll that is located in the same folder as an ISP file.  
  
[CVE-2010-3143] Untrusted search path vulnerability in Microsoft Windows Contacts allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse wab32res.dll that is located in the same folder as a .contact, .group, .p7c, .vcf, or .wab file. NOTE: the codebase for this product may overlap the codebase for the product referenced in CVE-2010-3147.  
  
[CVE-2010-3144] "Untrusted search path vulnerability in the Internet Connection Signup Wizard in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse smmscrpt.dll file in the current working directory, as demonstrated by a directory that contains an ISP or INS file, aka ""Internet Connection Signup Wizard Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3145] "Untrusted search path vulnerability in the BitLocker Drive Encryption API, as used in sdclt.exe in Backup Manager in Microsoft Windows Vista SP1 and SP2, allows local users to gain privileges via a Trojan horse fveapi.dll file in the current working directory, as demonstrated by a directory that contains a Windows Backup Catalog (.wbcat) file, aka ""Backup Manager Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3147] "Untrusted search path vulnerability in wab.exe 6.00.2900.5512 in Windows Address Book in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a Trojan horse wab32res.dll file in the current working directory, as demonstrated by a directory that contains a Windows Address Book (WAB), VCF (aka vCard), or P7C file, aka ""Insecure Library Loading Vulnerability."" NOTE: the codebase for this product may overlap the codebase for the product referenced in CVE-2010-3143."  
  
[CVE-2010-3223] "The user interface in Microsoft Cluster Service (MSCS) in Microsoft Windows Server 2008 R2 does not properly set administrative-share permissions for new cluster disks that are shared as part of a failover cluster, which allows remote attackers to read or modify data on these disks via requests to the associated share, aka ""Permissions on New Cluster Disks Vulnerability."""  
  
[CVE-2010-3225] "Use-after-free vulnerability in the Media Player Network Sharing Service in Microsoft Windows Vista SP1 and SP2 and Windows 7 allows remote attackers to execute arbitrary code via a crafted Real Time Streaming Protocol (RTSP) packet, aka ""RTSP Use After Free Vulnerability."""  
  
[CVE-2010-3227] "Stack-based buffer overflow in the UpdateFrameTitleForDocument method in the CFrameWnd class in mfc42.dll in the Microsoft Foundation Class (MFC) Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows context-dependent attackers to execute arbitrary code via a long window title that this library attempts to create at the request of an application, as demonstrated by the Trident PowerZip 7.2 Build 4010 application, aka ""Windows MFC Document Title Updating Buffer Overflow Vulnerability."""  
  
[CVE-2010-3229] "The Secure Channel (aka SChannel) security package in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when IIS 7.x is used, does not properly process client certificates during SSL and TLS handshakes, which allows remote attackers to cause a denial of service (LSASS outage and reboot) via a crafted packet, aka ""TLSv1 Denial of Service Vulnerability."""  
  
[CVE-2010-3243] "Cross-site scripting (XSS) vulnerability in the toStaticHTML function in Microsoft Internet Explorer 8, and the SafeHTML function in Microsoft Windows SharePoint Services 3.0 SP2 and Office SharePoint Server 2007 SP2, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka ""HTML Sanitization Vulnerability."""  
  
[CVE-2010-3324] "The toStaticHTML function in Microsoft Internet Explorer 8, and the SafeHTML function in Microsoft Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010, Office SharePoint Server 2007 SP2, Groove Server 2010, and Office Web Apps, allows remote attackers to bypass the cross-site scripting (XSS) protection mechanism and conduct XSS attacks via a crafted use of the Cascading Style Sheets (CSS) @import rule, aka ""HTML Sanitization Vulnerability,"" a different vulnerability than CVE-2010-1257."  
  
[CVE-2010-3338] "The Windows Task Scheduler in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the security context of scheduled tasks, which allows local users to gain privileges via a crafted application, aka ""Task Scheduler Vulnerability."" NOTE: this might overlap CVE-2010-3888."  
  
[CVE-2010-3888] Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Kaspersky Lab researchers and other researchers.  
  
[CVE-2010-3889] Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Microsoft researchers and other researchers.  
  
[CVE-2010-3937] "Microsoft Exchange Server 2007 SP2 on the x64 platform allows remote authenticated users to cause a denial of service (infinite loop and MSExchangeIS outage) via a crafted RPC request, aka ""Exchange Server Infinite Loop Vulnerability."""  
  
[CVE-2010-3939] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via vectors related to improper memory allocation for copies from user mode, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2010-3940] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted application, aka ""Win32k PFE Pointer Double Free Vulnerability."""  
  
[CVE-2010-3941] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold and SP2, and Windows 7 allows local users to gain privileges via a crafted application, aka ""Win32k Double Free Vulnerability."""  
  
[CVE-2010-3942] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for copies from user mode, which allows local users to gain privileges via a crafted application, aka ""Win32k WriteAV Vulnerability."""  
  
[CVE-2010-3943] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly link driver objects, which allows local users to gain privileges via a crafted application that triggers linked-list corruption, aka ""Win32k Cursor Linking Vulnerability."""  
  
[CVE-2010-3944] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2010-3956] "The OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly perform array indexing, which allows local users to gain privileges via a crafted OpenType font, aka ""OpenType Font Index Vulnerability."""  
  
[CVE-2010-3957] "Double free vulnerability in the OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted OpenType font, aka ""OpenType Font Double Free Vulnerability."""  
  
[CVE-2010-3959] "The OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted CMAP table in an OpenType font, aka ""OpenType CMAP Table Vulnerability."""  
  
[CVE-2010-3960] "Hyper-V in Microsoft Windows Server 2008 Gold, SP2, and R2 allows guest OS users to cause a denial of service (host OS hang) by sending a crafted encapsulated packet over the VMBus, aka ""Hyper-V VMBus Vulnerability."""  
  
[CVE-2010-3961] "The Consent User Interface (UI) in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly handle an unspecified registry-key value, which allows local users with SeImpersonatePrivilege rights to gain privileges via a crafted application, aka ""Consent UI Impersonation Vulnerability."""  
  
[CVE-2010-3963] "Buffer overflow in the Routing and Remote Access NDProxy component in the kernel in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted application, related to the Routing and Remote Access service (RRAS) and improper copying from user mode to the kernel, aka ""Kernel NDProxy Buffer Overflow Vulnerability."""  
  
[CVE-2010-3965] "Untrusted search path vulnerability in Windows Media Encoder 9 on Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Windows Media Profile (PRX) file, aka ""Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3966] "Untrusted search path vulnerability in Microsoft Windows Server 2008 R2 and Windows 7, when BranchCache is supported, allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an EML file, an RSS file, or a WPOST file, aka ""BranchCache Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3967] "Untrusted search path vulnerability in Microsoft Windows Movie Maker (WMM) 2.6 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Movie Maker (MSWMM) file, aka ""Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3970] "Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Windows Shell graphics processor (aka graphics rendering engine) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unspecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao, aka ""Windows Shell Graphics Processing Overrun Vulnerability."""  
  
[CVE-2010-3973] "The WMITools ActiveX control in WBEMSingleView.ocx 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via a crafted argument to the AddContextRef method, possibly an untrusted pointer dereference, aka ""Microsoft WMITools ActiveX Control Vulnerability."""  
  
[CVE-2010-3974] "fxscover.exe in the Fax Cover Page Editor in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly parse FAX cover pages, which allows remote attackers to execute arbitrary code via a crafted .cov file, aka ""Fax Cover Page Editor Memory Corruption Vulnerability."""  
  
[CVE-2010-4182] "Untrusted search path vulnerability in the Data Access Objects (DAO) library (dao360.dll) in Microsoft Windows XP Professional SP3, Windows Server 2003 R2 Enterprise Edition SP3, Windows Vista Business SP1, and Windows 7 Professional allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse msjet49.dll that is located in the same folder as a file that is processed by dao360.dll. NOTE: the provenance of this information is unknown  
[CVE-2010-4398] "Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG\_BINARY value for a SystemDefaultEUDCFont registry key, aka ""Driver Improper Interaction with Windows Kernel Vulnerability."""  
  
[CVE-2010-4562] Microsoft Windows 2008, 7, Vista, 2003, 2000, and XP, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping. NOTE: due to a typo, some sources map CVE-2010-4562 to a ProFTPd mod\_sql vulnerability, but that issue is covered by CVE-2010-4652.  
  
[CVE-2010-4669] The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 allows remote attackers to cause a denial of service (CPU consumption and system hang) by sending many Router Advertisement (RA) messages with different source addresses, as demonstrated by the flood\_router6 program in the thc-ipv6 package.  
  
[CVE-2010-4701] Heap-based buffer overflow in the CDrawPoly::Serialize function in fxscover.exe in Microsoft Windows Fax Services Cover Page Editor 5.2 r2 in Windows XP Professional SP3, Server 2003 R2 Enterprise Edition SP2, and Windows 7 Professional allows remote attackers to execute arbitrary code via a long record in a Fax Cover Page (.cov) file. NOTE: some of these details are obtained from third party information.  
  
[CVE-2010-5082] "Untrusted search path vulnerability in colorcpl.exe 6.0.6000.16386 in the Color Control Panel in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 allows local users to gain privileges via a Trojan horse sti.dll file in the current working directory, as demonstrated by a directory that contains a .camp, .cdmp, .gmmp, .icc, or .icm file, aka ""Color Control Panel Insecure Library Loading Vulnerability."""  
  
[CVE-2011-0026] "Integer signedness error in the SQLConnectW function in an ODBC API (odbc32.dll) in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, allows remote attackers to execute arbitrary code via a long string in the Data Source Name (DSN) and a crafted szDSN argument, which bypasses a signed comparison and leads to a buffer overflow, aka ""DSN Overflow Vulnerability."""  
  
[CVE-2011-0027] "Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, does not properly validate memory allocation for internal data structures, which allows remote attackers to execute arbitrary code, possibly via a large CacheSize property that triggers an integer wrap and a buffer overflow, aka ""ADO Record Memory Vulnerability."" NOTE: this might be a duplicate of CVE-2010-1117 or CVE-2010-1118."  
  
[CVE-2011-0028] "WordPad in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly parse fields in Word documents, which allows remote attackers to execute arbitrary code via a crafted .doc file, aka ""WordPad Converter Parsing Vulnerability."""  
  
[CVE-2011-0030] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly kill processes after a logout, which allows local users to obtain sensitive information or gain privileges via a crafted application that continues to execute throughout the logout of one user and the login session of the next user, aka ""CSRSS Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2010-0023."  
  
[CVE-2011-0031] "The (1) JScript 5.8 and (2) VBScript 5.8 scripting engines in Microsoft Windows Server 2008 R2 and Windows 7 do not properly load decoded scripts obtained from web pages, which allows remote attackers to trigger memory corruption and consequently obtain sensitive information via a crafted web site, aka ""Scripting Engines Information Disclosure Vulnerability."""  
  
[CVE-2011-0032] "Untrusted search path vulnerability in DirectShow in Microsoft Windows Vista SP1 and SP2, Windows 7 Gold and SP1, Windows Server 2008 R2 and R2 SP1, and Windows Media Center TV Pack for Windows Vista allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Digital Video Recording (.dvr-ms), Windows Recorded TV Show (.wtv), or .mpg file, aka ""DirectShow Insecure Library Loading Vulnerability."""  
  
[CVE-2011-0033] "The OpenType Compact Font Format (CFF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate parameter values in OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted font, aka ""OpenType Font Encoded Character Vulnerability."""  
  
[CVE-2011-0034] "Stack-based buffer overflow in the OpenType Compact Font Format (aka OTF or CFF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via crafted parameter values in an OpenType font, aka ""OpenType Font Stack Overflow Vulnerability."""  
  
[CVE-2011-0037] Microsoft Malware Protection Engine before 1.1.6603.0, as used in Microsoft Malicious Software Removal Tool (MSRT), Windows Defender, Security Essentials, Forefront Client Security, Forefront Endpoint Protection 2010, and Windows Live OneCare, allows local users to gain privileges via a crafted value of an unspecified user registry key.  
  
[CVE-2011-0039] "The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly process authentication requests, which allows local users to gain privileges via a request with a crafted length, aka ""LSASS Length Validation Vulnerability."""  
  
[CVE-2011-0040] "The server in Microsoft Active Directory on Windows Server 2003 SP2 does not properly handle an update request for a service principal name (SPN), which allows remote attackers to cause a denial of service (authentication downgrade or outage) via a crafted request that triggers name collisions, aka ""Active Directory SPN Validation Vulnerability."""  
  
[CVE-2011-0041] "Integer overflow in gdiplus.dll in GDI+ in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold and SP2, and Office XP SP3 allows remote attackers to execute arbitrary code via a crafted EMF image, aka ""GDI+ Integer Overflow Vulnerability."""  
  
[CVE-2011-0042] "SBE.dll in the Stream Buffer Engine in Windows Media Player and Windows Media Center in Microsoft Windows XP SP2 and SP3, Windows XP Media Center Edition 2005 SP3, Windows Vista SP1 and SP2, Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista does not properly parse Digital Video Recording (.dvr-ms) files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""DVR-MS Vulnerability."""  
  
[CVE-2011-0043] "Kerberos in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 supports weak hashing algorithms, which allows local users to gain privileges by operating a service that sends crafted service tickets, as demonstrated by the CRC32 algorithm, aka ""Kerberos Unkeyed Checksum Vulnerability."""  
  
[CVE-2011-0045] "The Trace Events functionality in the kernel in Microsoft Windows XP SP3 does not properly perform type conversion, which causes integer truncation and insufficient memory allocation and triggers a buffer overflow, which allows local users to gain privileges via a crafted application, related to WmiTraceMessageVa, aka ""Windows Kernel Integer Truncation Vulnerability."""  
  
[CVE-2011-0086] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Improper User Input Validation Vulnerability."""  
  
[CVE-2011-0087] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Insufficient User Input Validation Vulnerability."""  
  
[CVE-2011-0088] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Class Pointer Confusion Vulnerability."""  
  
[CVE-2011-0089] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Class Improper Pointer Validation Vulnerability."""  
  
[CVE-2011-0090] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2011-0091] "Kerberos in Microsoft Windows Server 2008 R2 and Windows 7 does not prevent a session from changing from strong encryption to DES encryption, which allows man-in-the-middle attackers to spoof network traffic and obtain sensitive information via a DES downgrade, aka ""Kerberos Spoofing Vulnerability."""  
  
[CVE-2011-0096] "The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for content blocks in a document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site that is visited in Internet Explorer, aka ""MHTML Mime-Formatted Request Vulnerability."""  
  
[CVE-2011-0347] Microsoft Internet Explorer on Windows XP allows remote attackers to trigger an incorrect GUI display and have unspecified other impact via vectors related to the DOM implementation, as demonstrated by cross\_fuzz.  
  
[CVE-2011-0627] Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.  
  
[CVE-2011-0638] Microsoft Windows does not properly warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.  
  
[CVE-2011-0654] "Integer underflow in the BowserWriteErrorLogEntry function in the Common Internet File System (CIFS) browser service in Mrxsmb.sys or bowser.sys in Active Directory in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via a malformed BROWSER ELECTION message, leading to a heap-based buffer overflow, aka ""Browser Pool Corruption Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2011-0657] "DNSAPI.dll in the DNS client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process DNS queries, which allows remote attackers to execute arbitrary code via (1) a crafted LLMNR broadcast query or (2) a crafted application, aka ""DNS Query Vulnerability."""  
  
[CVE-2011-0658] "Integer underflow in the OLE Automation protocol implementation in VBScript.dll in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted WMF file, aka ""OLE Automation Underflow Vulnerability."""  
  
[CVE-2011-0660] "The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Response Parsing Vulnerability."""  
  
[CVE-2011-0661] "The SMB Server service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet, aka ""SMB Transaction Parsing Vulnerability."""  
  
[CVE-2011-0662] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0665] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0666] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0667] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0670] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0671] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0672] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0673] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-0674] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0675] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0676] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-0677] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1068] Microsoft Windows Azure Software Development Kit (SDK) 1.3.x before 1.3.20121.1237, when Full IIS and a Web Role are used with an ASP.NET application, does not properly support the use of cookies for maintaining state, which allows remote attackers to obtain potentially sensitive information by reading an encrypted cookie and performing unspecified other steps.  
  
[CVE-2011-1225] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1226] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1227] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1228] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1229] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1230] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1231] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1232] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1233] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1234] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1235] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1236] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1237] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1238] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1239] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1240] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1241] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1242] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1243] "The Windows Messenger ActiveX control in msgsc.dll in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via unspecified vectors that ""corrupt the system state,"" aka ""Microsoft Windows Messenger ActiveX Control Vulnerability."""  
  
[CVE-2011-1247] "Untrusted search path vulnerability in the Microsoft Active Accessibility component in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Active Accessibility Insecure Library Loading Vulnerability."""  
  
[CVE-2011-1248] "WINS in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1 does not properly handle socket send exceptions, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted packets, related to unintended stack-frame values and buffer passing, aka ""WINS Service Failed Response Vulnerability."""  
  
[CVE-2011-1249] "The Ancillary Function Driver (AFD) in afd.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1252] "Cross-site scripting (XSS) vulnerability in the SafeHTML function in the toStaticHTML API in Microsoft Internet Explorer 7 and 8, Office SharePoint Server 2007 SP2, Office SharePoint Server 2010 Gold and SP1, Groove Server 2010 Gold and SP1, Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1 allows remote attackers to inject arbitrary web script or HTML via unspecified strings, aka ""toStaticHTML Information Disclosure Vulnerability"" or ""HTML Sanitization Vulnerability."""  
  
[CVE-2011-1263] "Cross-site scripting (XSS) vulnerability in the logon page in Remote Desktop Web Access (RD Web Access) in Microsoft Windows Server 2008 R2 and R2 SP1 allows remote attackers to inject arbitrary web script or HTML via the URI, aka ""Remote Desktop Web Access Vulnerability."""  
  
[CVE-2011-1264] "Cross-site scripting (XSS) vulnerability in Active Directory Certificate Services Web Enrollment in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1 allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka ""Active Directory Certificate Services Vulnerability."""  
  
[CVE-2011-1265] "The Bluetooth Stack 2.1 in Microsoft Windows Vista SP1 and SP2 and Windows 7 Gold and SP1 does not prevent access to objects in memory that (1) were not properly initialized or (2) have been deleted, which allows remote attackers to execute arbitrary code via crafted Bluetooth packets, aka ""Bluetooth Stack Vulnerability."""  
  
[CVE-2011-1267] "The SMB server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 request, aka ""SMB Request Parsing Vulnerability."""  
  
[CVE-2011-1268] "The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Response Parsing Vulnerability."""  
  
[CVE-2011-1281] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly restrict the number of console objects for a process, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP AllocConsole Vulnerability."""  
  
[CVE-2011-1282] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly initialize memory and consequently uses a NULL pointer in an unspecified function call, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvSetConsoleLocalEUDC Vulnerability."""  
  
[CVE-2011-1283] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 does not ensure that an unspecified array index has a non-negative value before performing read and write operations, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvSetConsoleNumberOfCommand Vulnerability."""  
  
[CVE-2011-1284] "Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvWriteConsoleOutput Vulnerability."""  
  
[CVE-2011-1346] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors, as demonstrated by Stephen Fewer as the second of three chained vulnerabilities during a Pwn2Own competition at CanSecWest 2011.  
  
[CVE-2011-1347] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to bypass Protected Mode and create arbitrary files by leveraging access to a Low integrity process, as demonstrated by Stephen Fewer as the third of three chained vulnerabilities during a Pwn2Own competition at CanSecWest 2011.  
  
[CVE-2011-1652] "\*\* DISPUTED \*\* The default configuration of Microsoft Windows 7 immediately prefers a new IPv6 and DHCPv6 service over a currently used IPv4 and DHCPv4 service upon receipt of an IPv6 Router Advertisement (RA), and does not provide an option to ignore an unexpected RA, which allows remote attackers to conduct man-in-the-middle attacks on communication with external IPv4 servers via vectors involving RAs, a DHCPv6 server, and NAT-PT on the local network, aka a ""SLAAC Attack."" NOTE: it can be argued that preferring IPv6 complies with RFC 3484, and that attempting to determine the legitimacy of an RA is currently outside the scope of recommended behavior of host operating systems."  
  
[CVE-2011-1713] Microsoft msxml.dll, as used in Internet Explorer 8 on Windows 7, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function. NOTE: this might overlap CVE-2011-1202.  
  
[CVE-2011-1868] "The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate fields in DFS responses, which allows remote DFS servers to execute arbitrary code via a crafted response, aka ""DFS Memory Corruption Vulnerability."""  
  
[CVE-2011-1869] "The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote DFS servers to cause a denial of service (system hang) via a crafted referral response, aka ""DFS Referral Response Vulnerability."""  
  
[CVE-2011-1870] "Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvWriteConsoleOutputString Vulnerability."""  
  
[CVE-2011-1871] "Tcpip.sys in the TCP/IP stack in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a series of crafted ICMP messages, aka ""ICMP Denial of Service Vulnerability."""  
  
[CVE-2011-1872] "Hyper-V in Microsoft Windows Server 2008 Gold, SP2, R2, and R2 SP1 allows guest OS users to cause a denial of service (host OS infinite loop) via malformed machine instructions in a VMBus packet, aka ""VMBus Persistent DoS Vulnerability."""  
  
[CVE-2011-1873] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 on 64-bit platforms does not properly validate pointers during the parsing of OpenType (aka OTF) fonts, which allows remote attackers to execute arbitrary code via a crafted font file, aka ""Win32k OTF Validation Vulnerability."""  
  
[CVE-2011-1874] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1875] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1876] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1877] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1878] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1879] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1880] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1881] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1882] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1883] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1884] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1885] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1886] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 does not properly validate the arguments to functions, which allows local users to read arbitrary data from kernel memory via a crafted application that triggers a NULL pointer dereference, aka ""Win32k Incorrect Parameter Validation Allows Information Disclosure Vulnerability."""  
  
[CVE-2011-1887] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1888] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1891] "Cross-site scripting (XSS) vulnerability in Microsoft Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters in a request to a script, aka ""Contact Details Reflected XSS Vulnerability."""  
  
[CVE-2011-1892] "Microsoft Office Groove 2007 SP2, SharePoint Workspace 2010 Gold and SP1, Office Forms Server 2007 SP2, Office SharePoint Server 2007 SP2, Office SharePoint Server 2010 Gold and SP1, Office Groove Data Bridge Server 2007 SP2, Office Groove Management Server 2007 SP2, Groove Server 2010 Gold and SP1, Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010, and Office Web Apps 2010 Gold and SP1 do not properly handle Web Parts containing XML classes referencing external entities, which allows remote authenticated users to read arbitrary files via a crafted XML and XSL file, aka ""SharePoint Remote File Disclosure Vulnerability."""  
  
[CVE-2011-1893] "Cross-site scripting (XSS) vulnerability in Microsoft Office SharePoint Server 2010, Windows SharePoint Services 2.0 and 3.0 SP2, and SharePoint Foundation 2010 allows remote attackers to inject arbitrary web script or HTML via the URI, aka ""SharePoint XSS Vulnerability."""  
  
[CVE-2011-1894] "The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for embedded content in an HTML document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted EMBED element in a web page that is visited in Internet Explorer, aka ""MHTML Mime-Formatted Request Vulnerability."""  
  
[CVE-2011-1965] "Tcpip.sys in the TCP/IP stack in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 does not properly implement URL-based QoS, which allows remote attackers to cause a denial of service (reboot) via a crafted URL to a web server, aka ""TCP/IP QOS Denial of Service Vulnerability."""  
  
[CVE-2011-1966] "The DNS server in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 does not properly handle NAPTR queries that trigger recursive processing, which allows remote attackers to execute arbitrary code via a crafted query, aka ""DNS NAPTR Query Vulnerability."""  
  
[CVE-2011-1967] "Winsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka ""CSRSS Vulnerability."""  
  
[CVE-2011-1968] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly process packets in memory, which allows remote attackers to cause a denial of service (reboot) by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, as exploited in the wild in 2011, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2011-1970] "The DNS server in Microsoft Windows Server 2003 SP2 and Windows Server 2008 SP2, R2, and R2 SP1 does not properly initialize memory, which allows remote attackers to cause a denial of service (service outage) via a query for a nonexistent domain, aka ""DNS Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2011-1971] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly parse file metadata, which allows local users to cause a denial of service (reboot) via a crafted file, aka ""Windows Kernel Metadata Parsing DOS Vulnerability."""  
  
[CVE-2011-1974] "NDISTAPI.sys in the NDISTAPI driver in Remote Access Service (RAS) in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""NDISTAPI Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1975] "Untrusted search path vulnerability in the Data Access Tracing component in Windows Data Access Components (Windows DAC) 6.0 in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an Excel .xlsx file, aka ""Data Access Components Insecure Library Loading Vulnerability."""  
  
[CVE-2011-1984] "WINS in Microsoft Windows Server 2003 SP2 and Server 2008 SP2, R2, and R2 SP1 allows local users to gain privileges by sending crafted packets over the loopback interface, aka ""WINS Local Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1985] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1991] "Multiple untrusted search path vulnerabilities in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .doc, .rtf, or .txt file, related to (1) deskpan.dll in the Display Panning CPL Extension, (2) EAPHost Authenticator Service, (3) Folder Redirection, (4) HyperTerminal, (5) the Japanese Input Method Editor (IME), and (6) Microsoft Management Console (MMC), aka ""Windows Components Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2002] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle TrueType fonts, which allows local users to cause a denial of service (system hang) via a crafted font file, aka ""Win32k TrueType Font Type Translation Vulnerability."""  
  
[CVE-2011-2003] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .fon file, aka ""Font Library File Buffer Overrun Vulnerability."""  
  
[CVE-2011-2004] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a crafted TrueType font file, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2011-3402."  
  
[CVE-2011-2005] "afd.sys in the Ancillary Function Driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2011-2009] "Untrusted search path vulnerability in Windows Media Center in Microsoft Windows Vista SP2 and Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista, allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Media Center Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2011] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-2013] "Integer overflow in the TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code by sending a sequence of crafted UDP packets to a closed port, aka ""Reference Counter Overflow Vulnerability."""  
  
[CVE-2011-2014] "The LDAP over SSL (aka LDAPS) implementation in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not examine Certificate Revocation Lists (CRLs), which allows remote authenticated users to bypass intended certificate restrictions and access Active Directory resources by leveraging a revoked X.509 certificate for a domain account, aka ""LDAPS Authentication Bypass Vulnerability."""  
  
[CVE-2011-2016] "Untrusted search path vulnerability in Windows Mail and Windows Meeting Space in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .eml or .wcinv file, aka ""Windows Mail Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2018] "The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 Gold and SP1 does not properly initialize objects, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2011-2019] "Untrusted search path vulnerability in Microsoft Internet Explorer 9 on Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an HTML file, aka ""Internet Explorer Insecure Library Loading Vulnerability."""  
  
[CVE-2011-3389] "The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a ""BEAST"" attack."  
  
[CVE-2011-3397] "The Microsoft Time component in DATIME.DLL in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted web site that leverages an unspecified ""binary behavior"" in Internet Explorer, aka ""Microsoft Time Remote Code Execution Vulnerability."""  
  
[CVE-2011-3400] "Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 do not properly handle OLE objects in memory, which allows remote attackers to execute arbitrary code via a crafted object in a file, aka ""OLE Property Vulnerability."""  
  
[CVE-2011-3401] "ENCDEC.DLL in Windows Media Player and Media Center in Microsoft Windows XP SP2 and SP3, Windows Vista SP2, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .dvr-ms file, aka ""Windows Media Player DVR-MS Memory Corruption Vulnerability."""  
  
[CVE-2011-3402] "Unspecified vulnerability in the TrueType font parsing engine in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via crafted font data in a Word document or web page, as exploited in the wild in November 2011 by Duqu, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2011-3406] "Buffer overflow in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote authenticated users to execute arbitrary code via a crafted query that leverages incorrect memory initialization, aka ""Active Directory Buffer Overflow Vulnerability."""  
  
[CVE-2011-3408] "Csrsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka ""CSRSS Local Privilege Elevation Vulnerability."""  
  
[CVE-2011-4434] Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 do not properly enforce AppLocker rules, which allows local users to bypass intended access restrictions via a (1) macro or (2) scripting feature in an application, as demonstrated by Microsoft Office applications and the SANDBOX\_INERT and LOAD\_IGNORE\_CODE\_AUTHZ\_LEVEL flags.  
  
[CVE-2011-4695] Unspecified vulnerability in Microsoft Windows 7 SP1, when Java is installed, allows local users to bypass Internet Explorer sandbox restrictions and gain privileges via unknown vectors, as demonstrated by the White Phosphorus wp\_ie\_sandbox\_escape module for Immunity CANVAS. NOTE: as of 20111207, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.  
  
[CVE-2011-5046] "The Graphics Device Interface (GDI) in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted data, as demonstrated by a large height attribute of an IFRAME element rendered by Safari, aka ""GDI Access Violation Vulnerability."""  
  
[CVE-2011-5279] CRLF injection vulnerability in the CGI implementation in Microsoft Internet Information Services (IIS) 4.x and 5.x on Windows NT and Windows 2000 allows remote attackers to modify arbitrary uppercase environment variables via a \n (newline) character in an HTTP header.  
  
[CVE-2012-0001] "The kernel in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly load structured exception handling tables, which allows context-dependent attackers to bypass the SafeSEH security feature by leveraging a Visual C++ .NET 2003 application, aka ""Windows Kernel SafeSEH Bypass Vulnerability."""  
  
[CVE-2012-0002] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2012-0003] "Unspecified vulnerability in winmm.dll in Windows Multimedia Library in Windows Media Player (WMP) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted MIDI file, aka ""MIDI Remote Code Execution Vulnerability."""  
  
[CVE-2012-0004] "Unspecified vulnerability in DirectShow in DirectX in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted media file, related to Quartz.dll, Qdvd.dll, closed captioning, and the Line21 DirectShow filter, aka ""DirectShow Remote Code Execution Vulnerability."""  
  
[CVE-2012-0005] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2, when a Chinese, Japanese, or Korean system locale is used, can access uninitialized memory during the processing of Unicode characters, which allows local users to gain privileges via a crafted application, aka ""CSRSS Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0006] "The DNS server in Microsoft Windows Server 2003 SP2 and Server 2008 SP2, R2, and R2 SP1 does not properly handle objects in memory during record lookup, which allows remote attackers to cause a denial of service (daemon restart) via a crafted query, aka ""DNS Denial of Service Vulnerability."""  
  
[CVE-2012-0009] "Untrusted search path vulnerability in the Windows Object Packager configuration in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse executable file in the current working directory, as demonstrated by a directory that contains a file with an embedded packaged object, aka ""Object Packager Insecure Executable Launching Vulnerability."""  
  
[CVE-2012-0013] "Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka ""Assembly Execution Vulnerability."""  
  
[CVE-2012-0148] "afd.sys in the Ancillary Function Driver in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 on 64-bit platforms does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""AfdPoll Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0149] "afd.sys in the Ancillary Function Driver in Microsoft Windows Server 2003 SP2 does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0150] "Buffer overflow in msvcrt.dll in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted media file, aka ""Msvcrt.dll Buffer Overflow Vulnerability."""  
  
[CVE-2012-0151] "The Authenticode Signature Verification function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly validate the digest of a signed portable executable (PE) file, which allows user-assisted remote attackers to execute arbitrary code via a modified file with additional content, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2012-0152] "The Remote Desktop Protocol (RDP) service in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka ""Terminal Server Denial of Service Vulnerability."""  
  
[CVE-2012-0154] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers keyboard layout errors, aka ""Keyboard Layout Use After Free Vulnerability."""  
  
[CVE-2012-0156] "DirectWrite in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly render Unicode characters, which allows remote attackers to cause a denial of service (application hang) via a (1) instant message or (2) web site, aka ""DirectWrite Application Denial of Service Vulnerability."""  
  
[CVE-2012-0157] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle window messaging, which allows local users to gain privileges via a crafted application that calls the PostMessage function, aka ""PostMessage Function Vulnerability."""  
  
[CVE-2012-0159] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview  
[CVE-2012-0164] "Microsoft .NET Framework 4 does not properly compare index values, which allows remote attackers to cause a denial of service (application hang) via crafted requests to a Windows Presentation Foundation (WPF) application, aka "".NET Framework Index Comparison Vulnerability."""  
  
[CVE-2012-0165] "GDI+ in Microsoft Windows Vista SP2 and Server 2008 SP2 and Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1 does not properly validate record types in EMF images, which allows remote attackers to execute arbitrary code via a crafted image, aka ""GDI+ Record Type Vulnerability."""  
  
[CVE-2012-0173] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka ""Remote Desktop Protocol Vulnerability,"" a different vulnerability than CVE-2012-0002."  
  
[CVE-2012-0174] "Windows Firewall in tcpip.sys in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly enforce firewall rules for outbound broadcast packets, which allows remote attackers to obtain potentially sensitive information by observing broadcast traffic on a local network, aka ""Windows Firewall Bypass Vulnerability."""  
  
[CVE-2012-0175] "The Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted name for a (1) file or (2) directory, aka ""Command Injection Vulnerability."""  
  
[CVE-2012-0176] "Double free vulnerability in Microsoft Silverlight 4 before 4.1.10329 on Windows allows remote attackers to execute arbitrary code via vectors involving crafted XAML glyphs, aka ""Silverlight Double-Free Vulnerability."""  
  
[CVE-2012-0178] "Race condition in partmgr.sys in Windows Partition Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that makes multiple simultaneous Plug and Play (PnP) Configuration Manager function calls, aka ""Plug and Play (PnP) Configuration Manager Vulnerability."""  
  
[CVE-2012-0179] "Double free vulnerability in tcpip.sys in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that binds an IPv6 address to a local interface, aka ""TCP/IP Double Free Vulnerability."""  
  
[CVE-2012-0180] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly handle user-mode input passed to kernel mode for (1) windows and (2) messages, which allows local users to gain privileges via a crafted application, aka ""Windows and Messages Vulnerability."""  
  
[CVE-2012-0181] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly manage Keyboard Layout files, which allows local users to gain privileges via a crafted application, aka ""Keyboard Layout File Vulnerability."""  
  
[CVE-2012-1194] "The resolver in the DNS Server service in Microsoft Windows Server 2008 before R2 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a ""ghost domain names"" attack."  
  
[CVE-2012-1527] "Integer underflow in Windows Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows local users to gain privileges via a crafted briefcase, aka ""Windows Briefcase Integer Underflow Vulnerability."""  
  
[CVE-2012-1528] "Integer overflow in Windows Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows local users to gain privileges via a crafted briefcase, aka ""Windows Briefcase Integer Overflow Vulnerability."""  
  
[CVE-2012-1537] "Heap-based buffer overflow in DirectPlay in DirectX 9.0 through 11.1 in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a crafted Office document, aka ""DirectPlay Heap Overflow Vulnerability."""  
  
[CVE-2012-1848] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly handle user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Scrollbar Calculation Vulnerability."""  
  
[CVE-2012-1850] "The Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle RAP responses, which allows remote attackers to cause a denial of service (service hang) via crafted RAP packets, aka ""Remote Administration Protocol Denial of Service Vulnerability."""  
  
[CVE-2012-1851] "Format string vulnerability in the Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted response, aka ""Print Spooler Service Format String Vulnerability."""  
  
[CVE-2012-1852] "Heap-based buffer overflow in the Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via crafted RAP response packets, aka ""Remote Administration Protocol Heap Overflow Vulnerability."""  
  
[CVE-2012-1853] "Stack-based buffer overflow in the Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP3 allows remote attackers to execute arbitrary code via crafted RAP response packets, aka ""Remote Administration Protocol Stack Overflow Vulnerability."""  
  
[CVE-2012-1863] "Cross-site scripting (XSS) vulnerability in Microsoft Office SharePoint Server 2007 SP2 and SP3 Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1 allows remote attackers to inject arbitrary web script or HTML via crafted JavaScript elements in a URL, aka ""SharePoint Reflected List Parameter Vulnerability."""  
  
[CVE-2012-1864] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""String Atom Class Name Handling Vulnerability,"" a different vulnerability than CVE-2012-1865."  
  
[CVE-2012-1865] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""String Atom Class Name Handling Vulnerability,"" a different vulnerability than CVE-2012-1864."  
  
[CVE-2012-1866] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""Clipboard Format Atom Name Handling Vulnerability."""  
  
[CVE-2012-1867] "Integer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted TrueType font file that triggers incorrect memory allocation, aka ""Font Resource Refcount Integer Overflow Vulnerability."""  
  
[CVE-2012-1868] "Race condition in the thread-creation implementation in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 allows local users to gain privileges via a crafted application, aka ""Win32k.sys Race Condition Vulnerability."""  
  
[CVE-2012-1870] "The CBC mode in the TLS protocol, as used in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and other products, allows remote web servers to obtain plaintext data by triggering multiple requests to a third-party HTTPS server and sniffing the network during the resulting HTTPS session, aka ""TLS Protocol Vulnerability."""  
  
[CVE-2012-1890] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle keyboard-layout files, which allows local users to gain privileges via a crafted application, aka ""Keyboard Layout Vulnerability."""  
  
[CVE-2012-1891] "Heap-based buffer overflow in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2 and Windows Data Access Components (WDAC) 6.0 allows remote attackers to execute arbitrary code via crafted XML data that triggers access to an uninitialized object in memory, aka ""ADO Cachesize Heap Overflow RCE Vulnerability."""  
  
[CVE-2012-1893] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate callback parameters during creation of a hook procedure, which allows local users to gain privileges via a crafted application, aka ""Win32k Incorrect Type Handling Vulnerability."""  
  
[CVE-2012-1945] Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allow local users to obtain sensitive information via an HTML document that loads a shortcut (aka .lnk) file for display within an IFRAME element, as demonstrated by a network share implemented by (1) Microsoft Windows or (2) Samba.  
  
[CVE-2012-2520] "Cross-site scripting (XSS) vulnerability in Microsoft InfoPath 2007 SP2 and SP3 and 2010 SP1, Communicator 2007 R2, Lync 2010 and 2010 Attendee, SharePoint Server 2007 SP2 and SP3 and 2010 SP1, Groove Server 2010 SP1, Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010 SP1, and Office Web Apps 2010 SP1 allows remote attackers to inject arbitrary web script or HTML via a crafted string, aka ""HTML Sanitization Vulnerability."""  
  
[CVE-2012-2526] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP3 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to a deleted object, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2012-2527] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2529] "Integer overflow in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Windows Kernel Integer Overflow Vulnerability."""  
  
[CVE-2012-2530] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2551] "The server in Kerberos in Microsoft Windows Server 2008 R2 and R2 SP1, and Windows 7 Gold and SP1, allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via a crafted session request, aka ""Kerberos NULL Dereference Vulnerability."""  
  
[CVE-2012-2553] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2556] "The OpenType Font (OTF) driver in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to execute arbitrary code via a crafted OpenType font file, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2012-2897] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT, as used by Google Chrome before 22.0.1229.79 and other programs, do not properly handle objects in memory, which allows remote attackers to execute arbitrary code via a crafted TrueType font file, aka ""Windows Font Parsing Vulnerability"" or ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2012-2971] The server in CA ARCserve Backup r12.5, r15, and r16 on Windows does not properly process RPC requests, which allows remote attackers to execute arbitrary code or cause a denial of service via a crafted request.  
  
[CVE-2012-2972] The (1) server and (2) agent components in CA ARCserve Backup r12.5, r15, and r16 on Windows do not properly validate RPC requests, which allows remote attackers to cause a denial of service (service crash) via a crafted request.  
  
[CVE-2012-2993] Microsoft Windows Phone 7 does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof an SSL server for the (1) POP3, (2) IMAP, or (3) SMTP protocol via an arbitrary valid certificate.  
  
[CVE-2012-4774] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow remote attackers to execute arbitrary code via a crafted (1) file name or (2) subfolder name that triggers use of unallocated memory as the destination of a copy operation, aka ""Windows Filename Parsing Vulnerability."""  
  
[CVE-2012-4786] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a crafted TrueType Font (TTF) file, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2012-5362] The IPv6 implementation in Microsoft Windows 7 and earlier allows remote attackers to cause a denial of service via a flood of ICMPv6 Neighbor Solicitation messages, a different vulnerability than CVE-2010-4669.  
  
[CVE-2012-5364] The IPv6 implementation in Microsoft Windows 7 and earlier allows remote attackers to cause a denial of service via a flood of ICMPv6 Router Advertisement packets containing multiple Routing entries.  
  
[CVE-2013-0001] "The Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 4, and 4.5 does not properly initialize memory arrays, which allows remote attackers to obtain sensitive information via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application that leverages a pointer to an unmanaged memory location, aka ""System Drawing Information Disclosure Vulnerability."""  
  
[CVE-2013-0002] "Buffer overflow in the Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application that leverages improper counting of objects during a memory copy operation, aka ""WinForms Buffer Overflow Vulnerability."""  
  
[CVE-2013-0005] "The WCF Replace function in the Open Data (aka OData) protocol implementation in Microsoft .NET Framework 3.5, 3.5 SP1, 3.5.1, and 4, and the Management OData IIS Extension on Windows Server 2012, allows remote attackers to cause a denial of service (resource consumption and daemon restart) via crafted values in HTTP requests, aka ""Replace Denial of Service Vulnerability."""  
  
[CVE-2013-0008] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle window broadcast messages, which allows local users to gain privileges via a crafted application, aka ""Win32k Improper Message Handling Vulnerability."""  
  
[CVE-2013-0011] "The Print Spooler in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted print job, aka ""Windows Print Spooler Components Vulnerability."""  
  
[CVE-2013-0013] "The SSL provider component in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle encrypted packets, which allows man-in-the-middle attackers to conduct SSLv2 downgrade attacks against (1) SSLv3 sessions or (2) TLS sessions by intercepting handshakes and injecting content, aka ""Microsoft SSL Version 3 and TLS Protocol Security Feature Bypass Vulnerability."""  
  
[CVE-2013-0073] "The Windows Forms (aka WinForms) component in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, and 4.5 does not properly restrict the privileges of a callback function during object creation, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application, aka ""WinForms Callback Elevation Vulnerability."""  
  
[CVE-2013-0075] "The TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (reboot) via a crafted packet that terminates a TCP connection, aka ""TCP FIN WAIT Vulnerability."""  
  
[CVE-2013-0076] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Reference Count Vulnerability."""  
  
[CVE-2013-0077] "Quartz.dll in DirectShow in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via crafted media content in (1) a media file, (2) a media stream, or (3) a Microsoft Office document, aka ""Media Decompression Vulnerability."""  
  
[CVE-2013-0078] "The Microsoft Antimalware Client in Windows Defender on Windows 8 and Windows RT uses an incorrect pathname for MsMpEng.exe, which allows local users to gain privileges via a crafted application, aka ""Microsoft Antimalware Improper Pathname Vulnerability."""  
  
[CVE-2013-0096] "Writer in Microsoft Windows Essentials 2011 and 2012 allows remote attackers to bypass proxy settings and overwrite arbitrary files via crafted URL parameters, aka ""Windows Essentials Improper URI Handling Vulnerability."""  
  
[CVE-2013-0810] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, and Windows Server 2008 SP2 allow remote attackers to execute arbitrary code via a crafted screensaver in a theme file, aka ""Windows Theme File Remote Code Execution Vulnerability."""  
  
[CVE-2013-0941] EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.  
  
[CVE-2013-1248] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1249] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1250] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1251] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1252] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1253] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1254] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1255] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1256] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1257] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1258] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1259] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1260] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1261] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1262] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1263] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1264] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1265] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1266] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1267] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1268] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1269] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1270] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1271] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1272] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1273] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1274] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1275] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1276] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1277] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1278] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages incorrect handling of objects in memory, aka ""Kernel Race Condition Vulnerability,"" a different vulnerability than CVE-2013-1279."  
  
[CVE-2013-1279] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages incorrect handling of objects in memory, aka ""Kernel Race Condition Vulnerability,"" a different vulnerability than CVE-2013-1278."  
  
[CVE-2013-1280] "The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Reference Count Vulnerability."""  
  
[CVE-2013-1281] "The NFS server in Microsoft Windows Server 2008 R2 and R2 SP1 and Server 2012 allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via an attempted renaming of a file or folder located on a read-only share, aka ""NULL Dereference Vulnerability."""  
  
[CVE-2013-1283] "Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Race Condition Vulnerability."""  
  
[CVE-2013-1284] "Race condition in the kernel in Microsoft Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Kernel Race Condition Vulnerability."""  
  
[CVE-2013-1285] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1286 and CVE-2013-1287."  
  
[CVE-2013-1286] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1285 and CVE-2013-1287."  
  
[CVE-2013-1287] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1285 and CVE-2013-1286."  
  
[CVE-2013-1291] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 Gold and SP1, and Windows 8 allows local users to cause a denial of service (reboot) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability"" or ""Win32k Font Parsing Vulnerability."""  
  
[CVE-2013-1292] "Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Race Condition Vulnerability."""  
  
[CVE-2013-1293] "The NTFS kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application that leverages improper handling of objects in memory, aka ""NTFS NULL Pointer Dereference Vulnerability."""  
  
[CVE-2013-1294] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Kernel Race Condition Vulnerability."""  
  
[CVE-2013-1295] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""CSRSS Memory Corruption Vulnerability."""  
  
[CVE-2013-1299] Microsoft Windows Modern Mail allows remote attackers to spoof link targets via a crafted HTML e-mail message.  
  
[CVE-2013-1300] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Allocation Vulnerability."""  
  
[CVE-2013-1305] "HTTP.sys in Microsoft Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (infinite loop) via a crafted HTTP header, aka ""HTTP.sys Denial of Service Vulnerability."""  
  
[CVE-2013-1313] "Object Linking and Embedding (OLE) Automation in Microsoft Windows XP SP3 does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted RTF document, aka ""OLE Automation Remote Code Execution Vulnerability."""  
  
[CVE-2013-1332] "dxgkrnl.sys (aka the DirectX graphics kernel subsystem) in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""DirectX Graphics Kernel Subsystem Double Fetch Vulnerability."""  
  
[CVE-2013-1333] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2013-1334] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Handle Vulnerability."""  
  
[CVE-2013-1337] "Microsoft .NET Framework 4.5 does not properly create policy requirements for custom Windows Communication Foundation (WCF) endpoint authentication in certain situations involving passwords over HTTPS, which allows remote attackers to bypass authentication by sending queries to an endpoint, aka ""Authentication Bypass Vulnerability."""  
  
[CVE-2013-1339] "The Print Spooler in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly manage memory during deletion of printer connections, which allows remote authenticated users to execute arbitrary code via a crafted request, aka ""Print Spooler Vulnerability."""  
  
[CVE-2013-1340] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Dereference Vulnerability."""  
  
[CVE-2013-1341] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 8 allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability."""  
  
[CVE-2013-1342] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1343] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1344, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1344] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1345] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Vulnerability."""  
  
[CVE-2013-2552] Unspecified vulnerability in Microsoft Internet Explorer 10 on Windows 8 allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a Medium integrity process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.  
  
[CVE-2013-2553] Unspecified vulnerability in the kernel in Microsoft Windows 7 allows local users to gain privileges via unknown vectors, as demonstrated by Nils and Jon of MWR Labs during a Pwn2Own competition at CanSecWest 2013, a different vulnerability than CVE-2013-0912.  
  
[CVE-2013-2554] Unspecified vulnerability in Microsoft Windows 7 allows attackers to bypass the ASLR and DEP protection mechanisms via unknown vectors, as demonstrated against Firefox by VUPEN during a Pwn2Own competition at CanSecWest 2013, a different vulnerability than CVE-2013-0787.  
  
[CVE-2013-2556] "Unspecified vulnerability in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 through SP1 allows attackers to bypass the ASLR protection mechanism via unknown vectors, as demonstrated against Adobe Flash Player by VUPEN during a Pwn2Own competition at CanSecWest 2013, aka ""ASLR Security Feature Bypass Vulnerability."""  
  
[CVE-2013-2558] Unspecified vulnerability in Microsoft Windows 8 allows remote attackers to cause a denial of service (reboot) or possibly have unknown other impact via a crafted TrueType Font (TTF) file, as demonstrated by the 120612-69701-01.dmp error report.  
  
[CVE-2013-3127] "The Microsoft WMV video codec in wmv9vcm.dll, wmvdmod.dll in Windows Media Format Runtime 9 and 9.5, and wmvdecod.dll in Windows Media Format Runtime 11 and Windows Media Player 11 and 12 allows remote attackers to execute arbitrary code via a crafted media file, aka ""WMV Video Decoder Remote Code Execution Vulnerability."""  
  
[CVE-2013-3128] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, and 4.5, allow remote attackers to execute arbitrary code via a crafted OpenType font (OTF) file, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2013-3136] "The kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly handle unspecified page-fault system calls, which allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Kernel Information Disclosure Vulnerability."""  
  
[CVE-2013-3138] "Integer overflow in the TCP/IP kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (system hang) via crafted TCP packets, aka ""TCP/IP Integer Overflow Vulnerability."""  
  
[CVE-2013-3154] "The signature-update functionality in Windows Defender on Microsoft Windows 7 and Windows Server 2008 R2 relies on an incorrect pathname, which allows local users to gain privileges via a Trojan horse application in the %SYSTEMDRIVE% top-level directory, aka ""Microsoft Windows 7 Defender Improper Pathname Vulnerability."""  
  
[CVE-2013-3167] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2013-3172] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to cause a denial of service (system hang) via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2013-3173] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overwrite Vulnerability."""  
  
[CVE-2013-3174] "DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a crafted GIF file, aka ""DirectShow Arbitrary Memory Overwrite Vulnerability."""  
  
[CVE-2013-3181] "usp10.dll in the Unicode Scripts Processor in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""Uniscribe Font Parsing Engine Memory Corruption Vulnerability."""  
  
[CVE-2013-3182] "The Windows NAT Driver (aka winnat) service in Microsoft Windows Server 2012 does not properly validate memory addresses during the processing of ICMP packets, which allows remote attackers to cause a denial of service (memory corruption and system hang) via crafted packets, aka ""Windows NAT Denial of Service Vulnerability."""  
  
[CVE-2013-3183] "The TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly perform memory allocation for inbound ICMPv6 packets, which allows remote attackers to cause a denial of service (system hang) via crafted packets, aka ""ICMPv6 Vulnerability."""  
  
[CVE-2013-3185] "Microsoft Active Directory Federation Services (AD FS) 1.x through 2.1 on Windows Server 2003 R2 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 allows remote attackers to obtain sensitive information about the service account, and possibly conduct account-lockout attacks, by connecting to an endpoint, aka ""AD FS Information Disclosure Vulnerability."""  
  
[CVE-2013-3186] "The Protected Mode feature in Microsoft Internet Explorer 7 through 10 on Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly implement the Integrity Access Level (aka IL) protection mechanism, which allows remote attackers to obtain medium-integrity privileges by leveraging access to a low-integrity process, aka ""Process Integrity Level Assignment Vulnerability."""  
  
[CVE-2013-3195] "The DSA\_InsertItem function in Comctl32.dll in the Windows common control library in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted value in an argument to an ASP.NET web application, aka ""Comctl32 Integer Overflow Vulnerability."""  
  
[CVE-2013-3196] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3197 and CVE-2013-3198."  
  
[CVE-2013-3197] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3196 and CVE-2013-3198."  
  
[CVE-2013-3198] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3196 and CVE-2013-3197."  
  
[CVE-2013-3200] "The USB drivers in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability."""  
  
[CVE-2013-3660] "The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 does not properly initialize a pointer for the next object in a certain list, which allows local users to obtain write access to the PATHRECORD chain, and consequently gain privileges, by triggering excessive consumption of paged memory and then making many FlattenPath function calls, aka ""Win32k Read AV Vulnerability."""  
  
[CVE-2013-3661] The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not check whether linked-list traversal is continually accessing the same list member, which allows local users to cause a denial of service (infinite traversal) via vectors that trigger a crafted PATHRECORD chain.  
  
[CVE-2013-3862] "Double free vulnerability in Microsoft Windows 7 and Server 2008 R2 SP1 allows local users to gain privileges via a crafted service description that is not properly handled by services.exe in the Service Control Manager (SCM), aka ""Service Control Manager Double Free Vulnerability."""  
  
[CVE-2013-3863] "Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allow remote attackers to execute arbitrary code via a crafted OLE object in a file, aka ""OLE Property Vulnerability."""  
  
[CVE-2013-3864] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, and CVE-2013-3865."  
  
[CVE-2013-3865] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, and CVE-2013-3864."  
  
[CVE-2013-3866] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2013-3868] "Microsoft Active Directory Lightweight Directory Service (AD LDS) on Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 8 and Active Directory Services on Windows Server 2008 SP2 and R2 SP1 and Server 2012 allow remote attackers to cause a denial of service (LDAP directory-service outage) via a crafted LDAP query, aka ""Remote Anonymous DoS Vulnerability."""  
  
[CVE-2013-3869] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to cause a denial of service (daemon hang) via a web-service request containing a crafted X.509 certificate that is not properly handled during validation, aka ""Digital Signatures Vulnerability."""  
  
[CVE-2013-3876] DirectAccess in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly verify server X.509 certificates, which allows man-in-the-middle attackers to spoof servers and read encrypted domain credentials via a crafted certificate.  
  
[CVE-2013-3879] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2013-3880] "The App Container feature in the kernel-mode drivers in Microsoft Windows 8, Windows Server 2012, and Windows RT allows remote attackers to bypass intended access restrictions and obtain sensitive information from a different container via a Trojan horse application, aka ""App Container Elevation of Privilege Vulnerability."""  
  
[CVE-2013-3881] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges via a crafted application, aka ""Win32k NULL Page Vulnerability."""  
  
[CVE-2013-3887] "The Ancillary Function Driver (AFD) in afd.sys in the kernel-mode drivers in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 allows local users to obtain sensitive information from kernel memory by leveraging improper copy operations, aka ""Ancillary Function Driver Information Disclosure Vulnerability."""  
  
[CVE-2013-3888] "dxgkrnl.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""DirectX Graphics Kernel Subsystem Double Fetch Vulnerability."""  
  
[CVE-2013-3894] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a crafted CMAP table in a TrueType font (TTF) file, aka ""TrueType Font CMAP Table Vulnerability."""  
  
[CVE-2013-3898] "Microsoft Windows 8 and Windows Server 2012, when Hyper-V is used, does not ensure memory-address validity, which allows guest OS users to execute arbitrary code in all guest OS instances, and allows guest OS users to cause a denial of service (host OS crash), via a guest-to-host hypercall with a crafted function parameter, aka ""Address Corruption Vulnerability."""  
  
[CVE-2013-3899] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate addresses, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2013-3900] "The WinVerifyTrust function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate PE file digests during Authenticode signature verification, which allows remote attackers to execute arbitrary code via a crafted PE file, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2013-3902] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1 and Windows 7 SP1 on 64-bit platforms allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2013-3903] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to cause a denial of service (reboot) via a crafted TrueType font (TTF) file, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2013-3906] "GDI+ in Microsoft Windows Vista SP2 and Server 2008 SP2  
[CVE-2013-3907] "portcls.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Port-Class Driver Double Fetch Vulnerability."""  
  
[CVE-2013-3918] "The InformationCardSigninHelper Class ActiveX control in icardie.dll in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted web page that is accessed by Internet Explorer, as exploited in the wild in November 2013, aka ""InformationCardSigninHelper Vulnerability."""  
  
[CVE-2013-3940] "Integer overflow in the Graphics Device Interface (GDI) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image in a Windows Write (.wri) document, which is not properly handled in WordPad, aka ""Graphics Device Interface Integer Overflow Vulnerability."""  
  
[CVE-2013-4858] Microsoft Windows Movie Maker 2.1.4026.0 on Windows XP SP3 allows remote attackers to cause a denial of service (application crash) via a crafted .wav file, as demonstrated by movieMaker.wav.  
  
[CVE-2013-5056] "Use-after-free vulnerability in the Scripting Runtime Object Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site that is visited with Internet Explorer, aka ""Use-After-Free Vulnerability in Microsoft Scripting Runtime Object Library."""  
  
[CVE-2013-5058] "Integer overflow in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows local users to gain privileges via a crafted application, aka ""Win32k Integer Overflow Vulnerability."""  
  
[CVE-2013-5065] NDProxy.sys in the kernel in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted application, as exploited in the wild in November 2013.  
  
[CVE-2013-6230] The Winsock WSAIoctl API in Microsoft Windows Server 2008, as used in ISC BIND 9.6-ESV before 9.6-ESV-R10-P1, 9.8 before 9.8.6-P1, 9.9 before 9.9.4-P1, 9.9.3-S1, 9.9.4-S1, and other products, does not properly support the SIO\_GET\_INTERFACE\_LIST command for netmask 255.255.255.255, which allows remote attackers to bypass intended IP address restrictions by leveraging misinterpretation of this netmask as a 0.0.0.0 netmask.  
  
[CVE-2013-6801] "Microsoft Word 2003 SP2 and SP3 on Windows XP SP3 allows remote attackers to cause a denial of service (CPU consumption) via a malformed .doc file containing an embedded image, as demonstrated by word2003forkbomb.doc, related to a ""fork bomb"" issue."  
  
[CVE-2013-6999] "\*\* DISPUTED \*\* The IsHandleEntrySecure function in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 SP2 does not properly validate the tagPROCESSINFO pW32Job field, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted NtUserValidateHandleSecure call for an owned object. NOTE: the vendor reportedly disputes the significance of this report, stating that ""it appears to be a local DOS ... we don't consider it a security vulnerability."""  
  
[CVE-2013-7331] The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers to determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes, as demonstrated by a res:// URL, and exploited in the wild in February 2014.  
  
[CVE-2013-7332] The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier does not properly detect recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.  
  
[CVE-2013-7369] SQL injection vulnerability in an unspecified DLL in the FSDBCom ActiveX control in F-Secure Anti-Virus for Microsoft Exchange Server before HF02, Anti-Virus for Windows Servers 9.00 before HF09, Anti-Virus for Citrix Servers 9.00 before HF09, and F-Secure Email and Server Security and F-Secure Server Security 9.20 before HF01 allows remote attackers to execute arbitrary SQL commands via unknown vectors, related to GetCommand.  
  
[CVE-2014-0251] "Microsoft Windows SharePoint Services 3.0 SP3  
[CVE-2014-0254] "The IPv6 implementation in Microsoft Windows 8, Windows Server 2012, and Windows RT does not properly validate packets, which allows remote attackers to cause a denial of service (system hang) via crafted ICMPv6 Router Advertisement packets, aka ""TCP/IP Version 6 (IPv6) Denial of Service Vulnerability."""  
  
[CVE-2014-0255] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka ""iSCSI Target Remote Denial of Service Vulnerability."""  
  
[CVE-2014-0256] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka ""iSCSI Target Remote Denial of Service Vulnerability."""  
  
[CVE-2014-0262] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 and Server 2008 R2 SP1 does not properly consider thread-owned objects during the processing of window handles, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Handle Vulnerability."""  
  
[CVE-2014-0263] "The Direct2D implementation in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a large 2D geometric figure that is encountered with Internet Explorer, aka ""Microsoft Graphics Component Memory Corruption Vulnerability."""  
  
[CVE-2014-0266] "The XMLHTTP ActiveX controls in XML Core Services 3.0 in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to bypass the Same Origin Policy via a web page that is visited in Internet Explorer, aka ""MSXML Information Disclosure Vulnerability."""  
  
[CVE-2014-0296] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly encrypt sessions, which makes it easier for man-in-the-middle attackers to obtain sensitive information by sniffing the network or modify session content by sending crafted RDP packets, aka ""RDP MAC Vulnerability."""  
  
[CVE-2014-0300] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2014-0301] "Double free vulnerability in qedit.dll in DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via a crafted JPEG image, aka ""DirectShow Memory Corruption Vulnerability."""  
  
[CVE-2014-0315] "Untrusted search path vulnerability in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a Trojan horse cmd.exe file in the current working directory, as demonstrated by a directory that contains a .bat or .cmd file, aka ""Windows File Handling Vulnerability."""  
  
[CVE-2014-0317] "The Security Account Manager Remote (SAMR) protocol implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2 does not properly determine the user-lockout state, which makes it easier for remote attackers to bypass the account lockout policy and obtain access via a brute-force attack, aka ""SAMR Security Feature Bypass Vulnerability."""  
  
[CVE-2014-0318] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly control access to thread-owned objects, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2014-0323] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (system hang) via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2014-1767] "Double free vulnerability in the Ancillary Function Driver (AFD) in afd.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2014-1807] "The ShellExecute API in Windows Shell in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly implement file associations, which allows local users to gain privileges via a crafted application, as exploited in the wild in May 2014, aka ""Windows Shell File Association Vulnerability."""  
  
[CVE-2014-1811] "The TCP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (non-paged pool memory consumption and system hang) via malformed data in the Options field of a TCP header, aka ""TCP Denial of Service Vulnerability."""  
  
[CVE-2014-1812] "The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka ""Group Policy Preferences Password Elevation of Privilege Vulnerability."""  
  
[CVE-2014-1814] "The Windows Installer in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application that invokes the repair feature for a different application, aka ""Windows Installer Repair Vulnerability."""  
  
[CVE-2014-1817] "usp10.dll in Uniscribe (aka the Unicode Script Processor) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted EMF+ record in a font file, aka ""Unicode Scripts Processor Vulnerability."""  
  
[CVE-2014-1818] "GDI+ in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code via a crafted EMF+ record in an image file, aka ""GDI+ Image Parsing Vulnerability."""  
  
[CVE-2014-1819] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly control access to objects associated with font files, which allows local users to gain privileges via a crafted file, aka ""Font Double-Fetch Vulnerability."""  
  
[CVE-2014-1824] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted Journal (aka .JNT) file, aka ""Windows Journal Remote Code Execution Vulnerability."""  
  
[CVE-2014-2671] Microsoft Windows Media Player (WMP) 11.0.5721.5230 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted WAV file.  
  
[CVE-2014-2780] "DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows local users to gain privileges by leveraging control over a low-integrity process to execute a crafted application, aka ""DirectShow Elevation of Privilege Vulnerability."""  
  
[CVE-2014-2781] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly restrict the exchange of keyboard and mouse data between programs at different integrity levels, which allows attackers to bypass intended access restrictions by leveraging control over a low-integrity process to launch the On-Screen Keyboard (OSK) and then upload a crafted application, aka ""On-Screen Keyboard Elevation of Privilege Vulnerability."""  
  
[CVE-2014-2814] "Microsoft Service Bus 1.1 on Microsoft Windows Server 2008 R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (AMQP messaging outage) via crafted AMQP messages, aka ""Service Bus Denial of Service Vulnerability."""  
  
[CVE-2014-4060] "Use-after-free vulnerability in MCPlayer.dll in Microsoft Windows Media Center TV Pack for Windows Vista, Windows 7 SP1, and Windows Media Center for Windows 8 and 8.1 allows remote attackers to execute arbitrary code via a crafted Office document that triggers deletion of a CSyncBasePlayer object, aka ""CSyncBasePlayer Use After Free Vulnerability."""  
  
[CVE-2014-4064] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly handle use of the paged kernel pool for allocation of uninitialized memory, which allows local users to obtain sensitive information about kernel addresses via a crafted application, aka ""Windows Kernel Pool Allocation Vulnerability."""  
  
[CVE-2014-4074] "The Task Scheduler in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via an application that schedules a crafted task, aka ""Task Scheduler Vulnerability."""  
  
[CVE-2014-4076] "Microsoft Windows Server 2003 SP2 allows local users to gain privileges via a crafted IOCTL call to (1) tcpip.sys or (2) tcpip6.sys, aka ""TCP/IP Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4077] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Office 2007 SP3, when IMJPDCT.EXE (aka IME for Japanese) is installed, allow remote attackers to bypass a sandbox protection mechanism via a crafted PDF document, aka ""Microsoft IME (Japanese) Elevation of Privilege Vulnerability,"" as exploited in the wild in 2014."  
  
[CVE-2014-4113] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, as exploited in the wild in October 2014, aka ""Win32k.sys Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4114] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a ""Sandworm"" attack in June through October 2014, aka ""Windows OLE Remote Code Execution Vulnerability."""  
  
[CVE-2014-4115] "fastfat.sys (aka the FASTFAT driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 does not properly allocate memory, which allows physically proximate attackers to execute arbitrary code or cause a denial of service (reserved-memory write) by connecting a crafted USB device, aka ""Microsoft Windows Disk Partition Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4118] "XML Core Services (aka MSXML) 3.0 in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (system-state corruption) via crafted XML content, aka ""MSXML Remote Code Execution Vulnerability."""  
  
[CVE-2014-4148] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted TrueType font, as exploited in the wild in October 2014, aka ""TrueType Font Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2014-4971] Microsoft Windows XP SP3 does not validate addresses in certain IRP handler routines, which allows local users to write data to arbitrary memory locations, and consequently gain privileges, via a crafted address in an IOCTL call, related to (1) the MQAC.sys driver in the MQ Access Control subsystem and (2) the BthPan.sys driver in the Bluetooth Personal Area Networking subsystem.  
  
[CVE-2014-6317] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (reboot) via a crafted TrueType font, aka ""Denial of Service in Windows Kernel Mode Driver Vulnerability."""  
  
[CVE-2014-6318] "The audit logon feature in Remote Desktop Protocol (RDP) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly log unauthorized login attempts supplying valid credentials, which makes it easier for remote attackers to bypass intended access restrictions via a series of attempts, aka ""Remote Desktop Protocol (RDP) Failure to Audit Vulnerability."""  
  
[CVE-2014-6321] "Schannel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via crafted packets, aka ""Microsoft Schannel Remote Code Execution Vulnerability."""  
  
[CVE-2014-6322] "The Windows Audio service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via a crafted web site, as demonstrated by execution of web script in Internet Explorer, aka ""Windows Audio Service Vulnerability."""  
  
[CVE-2014-6324] "The Kerberos Key Distribution Center (KDC) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote authenticated domain users to obtain domain administrator privileges via a forged signature in a ticket, as exploited in the wild in November 2014, aka ""Kerberos Checksum Vulnerability."""  
  
[CVE-2014-6332] "OleAut32.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted web site, as demonstrated by an array-redimensioning attempt that triggers improper handling of a size value in the SafeArrayDimen function, aka ""Windows OLE Automation Array Remote Code Execution Vulnerability."""  
  
[CVE-2014-6352] Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document.  
  
[CVE-2014-6355] "The Graphics Component in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly process JPEG images, which makes it easier for remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka ""Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2015-0001] "The Windows Error Reporting (WER) component in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to bypass the Protected Process Light protection mechanism and read the contents of arbitrary process-memory locations by leveraging administrative privileges, aka ""Windows Error Reporting Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0002] "The AhcVerifyAdminContext function in ahcache.sys in the Application Compatibility component in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not verify that an impersonation token is associated with an administrative account, which allows local users to gain privileges by running AppCompatCache.exe with a crafted DLL file, aka MSRC ID 20544 or ""Microsoft Application Compatibility Infrastructure Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0003] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0004] "The User Profile Service (aka ProfSvc) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges by conducting a junction attack to load another user's UsrClass.dat registry hive, aka MSRC ID 20674 or ""Microsoft User Profile Service Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0005] "The NETLOGON service in Microsoft Windows Server 2003 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2, when a Domain Controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, aka ""NETLOGON Spoofing Vulnerability."""  
  
[CVE-2015-0006] "The Network Location Awareness (NLA) service in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not perform mutual authentication to determine a domain connection, which allows remote attackers to trigger an unintended permissive configuration by spoofing DNS and LDAP responses on a local network, aka ""NLA Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0008] "The UNC implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not include authentication from the server to the client, which allows remote attackers to execute arbitrary code by making crafted data available on a UNC share, as demonstrated by Group Policy data from a spoofed domain controller, aka ""Group Policy Remote Code Execution Vulnerability."""  
  
[CVE-2015-0009] "The Group Policy Security Configuration policy implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows man-in-the-middle attackers to disable a signing requirement and trigger a revert-to-default action by spoofing domain-controller responses, aka ""Group Policy Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0010] "The CryptProtectMemory function in cng.sys (aka the Cryptography Next Generation driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1, when the CRYPTPROTECTMEMORY\_SAME\_LOGON option is used, does not check an impersonation token's level, which allows local users to bypass intended decryption restrictions by leveraging a service that (1) has a named-pipe planting vulnerability or (2) uses world-readable shared memory for encrypted data, aka ""CNG Security Feature Bypass Vulnerability"" or MSRC ID 20707."  
  
[CVE-2015-0011] "mrxdav.sys (aka the WebDAV driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to bypass an impersonation protection mechanism, and obtain privileges for redirection of WebDAV requests, via a crafted application, aka ""WebDAV Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0014] "Buffer overflow in the Telnet service in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted packets, aka ""Windows Telnet Service Buffer Overflow Vulnerability."""  
  
[CVE-2015-0015] "Microsoft Windows Server 2003 SP2, Server 2008 SP2 and R2 SP1, and Server 2012 Gold and R2 allow remote attackers to cause a denial of service (system hang and RADIUS outage) via crafted username strings to (1) Internet Authentication Service (IAS) or (2) Network Policy Server (NPS), aka ""Network Policy Server RADIUS Implementation Denial of Service Vulnerability."""  
  
[CVE-2015-0016] "Directory traversal vulnerability in the TS WebProxy (aka TSWbPrxy) component in Microsoft Windows Vista SP2, Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via a crafted pathname in an executable file, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""Directory Traversal Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0057] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0058] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows local users to gain privileges via a crafted application, aka ""Windows Cursor Object Double Free Vulnerability."""  
  
[CVE-2015-0059] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted TrueType font, aka ""TrueType Font Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2015-0060] "The font mapper in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly scale fonts, which allows local users to cause a denial of service (system hang) via a crafted application, aka ""Windows Font Driver Denial of Service Vulnerability."""  
  
[CVE-2015-0061] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize memory for TIFF images, which allows remote attackers to obtain sensitive information from process memory via a crafted image file, aka ""TIFF Processing Information Disclosure Vulnerability."""  
  
[CVE-2015-0062] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to gain privileges via a crafted application that leverages incorrect impersonation handling in a process that uses the SeAssignPrimaryTokenPrivilege privilege, aka ""Windows Create Process Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0073] "The Windows Registry Virtualization feature in the kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict changes to virtual stores, which allows local users to gain privileges via a crafted application, aka ""Registry Virtualization Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0074] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly allocate memory, which allows remote attackers to cause a denial of service via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Denial of Service Vulnerability."""  
  
[CVE-2015-0075] "The kernel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Impersonation Level Check Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0076] "The photo-decoder implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly initialize memory for rendering of JXR images, which allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""JPEG XR Parser Information Disclosure Vulnerability."""  
  
[CVE-2015-0077] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize function buffers, which allows local users to obtain sensitive information from kernel memory, and possibly bypass the ASLR protection mechanism, via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0078] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate the token of a calling thread, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0079] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to cause a denial of service (memory consumption and RDP outage) by establishing many RDP sessions that do not properly free allocated memory, aka ""Remote Desktop Protocol (RDP) Denial of Service Vulnerability."""  
  
[CVE-2015-0080] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize memory for rendering of malformed PNG images, which allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Malformed PNG Parsing Information Disclosure Vulnerability."""  
  
[CVE-2015-0081] "Windows Text Services (WTS) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""WTS Remote Code Execution Vulnerability."""  
  
[CVE-2015-0084] "The Task Scheduler in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to bypass intended restrictions on launching executable files via a crafted task, aka ""Task Scheduler Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0085] "Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Excel Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Server 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePoint Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, and SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka ""Microsoft Office Component Use After Free Vulnerability."""  
  
[CVE-2015-0087] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive information from kernel memory, and possibly bypass the KASLR protection mechanism, via a crafted font, aka ""Adobe Font Driver Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-0089."  
  
[CVE-2015-0088] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0089] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive information from kernel memory, and possibly bypass the KASLR protection mechanism, via a crafted font, aka ""Adobe Font Driver Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-0087."  
  
[CVE-2015-0090] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0091] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0092] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0093."  
  
[CVE-2015-0093] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0092."  
  
[CVE-2015-0094] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly restrict the availability of address information during a function call, which makes it easier for local users to bypass the ASLR protection mechanism via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0095] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to cause a denial of service (NULL pointer dereference and blue screen), or obtain sensitive information from kernel memory and possibly bypass the ASLR protection mechanism, via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0096] "Untrusted search path vulnerability in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, leading to DLL loading during Windows Explorer access to the icon of a crafted shortcut, aka ""DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-0098] "Task Scheduler in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges by triggering application execution by an invalid task, aka ""Task Scheduler Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1635] "HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka ""HTTP.sys Remote Code Execution Vulnerability."""  
  
[CVE-2015-1637] "Schannel (aka Secure Channel) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict TLS state transitions, which makes it easier for remote attackers to conduct cipher-downgrade attacks to EXPORT\_RSA ciphers via crafted TLS traffic, related to the ""FREAK"" issue, a different vulnerability than CVE-2015-0204 and CVE-2015-1067."  
  
[CVE-2015-1638] "Microsoft Active Directory Federation Services (AD FS) 3.0 on Windows Server 2012 R2 does not properly handle logoff actions, which allows remote attackers to bypass intended access restrictions by leveraging an unattended workstation, aka ""Active Directory Federation Services Information Disclosure Vulnerability."""  
  
[CVE-2015-1643] "Microsoft Windows Server 2003 R2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""NtCreateTransactionManager Type Confusion Vulnerability."""  
  
[CVE-2015-1644] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows MS-DOS Device Name Vulnerability."""  
  
[CVE-2015-1645] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to execute arbitrary code via a crafted Enhanced Metafile (EMF) image, aka ""EMF Processing Remote Code Execution Vulnerability."""  
  
[CVE-2015-1647] "Virtual Machine Manager (VMM) in Hyper-V in Microsoft Windows 8.1 and Windows Server 2012 R2 allows guest OS users to cause a denial of service (VMM functionality loss) via a crafted application, aka ""Windows Hyper-V DoS Vulnerability."""  
  
[CVE-2015-1670] "The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2, allows remote attackers to obtain sensitive information from process memory via a crafted OpenType font on a web site, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-1671] "The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2  
[CVE-2015-1673] "The Windows Forms (aka WinForms) libraries in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2 allow user-assisted remote attackers to execute arbitrary code via a crafted partial-trust application, aka ""Windows Forms Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1674] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate an unspecified address, which allows local users to bypass the KASLR protection mechanism, and consequently discover the cng.sys base address, via a crafted application, aka ""Windows Kernel Security Feature Bypass Vulnerability."""  
  
[CVE-2015-1675] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1676] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1677, CVE-2015-1678, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1677] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1678, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1678] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1679] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, and CVE-2015-1680."  
  
[CVE-2015-1680] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, and CVE-2015-1679."  
  
[CVE-2015-1681] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to cause a denial of service via a crafted .msc file, aka ""Microsoft Management Console File Format Denial of Service Vulnerability."""  
  
[CVE-2015-1695] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1696] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1697] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1698] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1699."  
  
[CVE-2015-1699] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1698."  
  
[CVE-2015-1701] "Win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows local users to gain privileges via a crafted application, as exploited in the wild in April 2015, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1702] "The Service Control Manager (SCM) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Service Control Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1716] "Schannel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict Diffie-Hellman Ephemeral (DHE) key lengths, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, aka ""Schannel Information Disclosure Vulnerability."""  
  
[CVE-2015-1719] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to obtain sensitive information from kernel memory via a crafted application, aka ""Microsoft Windows Kernel Information Disclosure Vulnerability."""  
  
[CVE-2015-1720] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Use After Free Vulnerability."""  
  
[CVE-2015-1721] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka ""Win32k Null Pointer Dereference Vulnerability."""  
  
[CVE-2015-1722] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Bitmap Handling Use After Free Vulnerability."""  
  
[CVE-2015-1723] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Station Use After Free Vulnerability."""  
  
[CVE-2015-1724] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Object Use After Free Vulnerability."""  
  
[CVE-2015-1725] "Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2015-1726] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Brush Object Use After Free Vulnerability."""  
  
[CVE-2015-1727] "Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Pool Buffer Overflow Vulnerability."""  
  
[CVE-2015-1728] "Microsoft Windows Media Player 10 through 12 allows remote attackers to execute arbitrary code via a crafted DataObject on a web site, aka ""Windows Media Player RCE via DataObject Vulnerability."""  
  
[CVE-2015-1756] "Use-after-free vulnerability in Microsoft Common Controls in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted web site that is accessed with the F12 Developer Tools feature of Internet Explorer, aka ""Microsoft Common Control Use After Free Vulnerability."""  
  
[CVE-2015-1757] "Cross-site scripting (XSS) vulnerability in adfs/ls in Active Directory Federation Services (AD FS) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 allows remote attackers to inject arbitrary web script or HTML via the wct parameter, aka ""ADFS XSS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1758] "Untrusted search path vulnerability in the LoadLibrary function in the kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a Trojan horse DLL in an unspecified directory, aka ""Windows LoadLibrary EoP Vulnerability."""  
  
[CVE-2015-1768] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1769] "Mount Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 mishandles symlinks, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Mount Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2360] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2361] "Hyper-V in Microsoft Windows 8.1 and Windows Server 2012 R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (buffer overflow) by leveraging guest OS privileges, aka ""Hyper-V Buffer Overflow Vulnerability."""  
  
[CVE-2015-2362] "Hyper-V in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS by leveraging guest OS privileges, aka ""Hyper-V System Data Structure Vulnerability."""  
  
[CVE-2015-2363] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2364] "The graphics component in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application that leverages an incorrect bitmap conversion, aka ""Graphics Component EOP Vulnerability."""  
  
[CVE-2015-2365] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2366] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2367] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from uninitialized kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2015-2368] "Untrusted search path vulnerability in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Windows DLL Remote Code Execution Vulnerability."""  
  
[CVE-2015-2369] "Untrusted search path vulnerability in Windows Media Device Manager in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rtf file, aka ""DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-2371] "The Windows Installer service in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a custom action script associated with a .msi package, aka ""Windows Installer EoP Vulnerability."""  
  
[CVE-2015-2373] "The Remote Desktop Protocol (RDP) server service in Microsoft Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a series of crafted packets, aka ""Remote Desktop Protocol (RDP) Remote Code Execution Vulnerability."""  
  
[CVE-2015-2374] "The Netlogon service in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2 does not properly implement domain-controller communication, which allows remote attackers to discover credentials by leveraging certain PDC access and spoofing the BDC role in a PDC communication channel, aka ""Elevation of Privilege Vulnerability in Netlogon."""  
  
[CVE-2015-2381] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-2382."  
  
[CVE-2015-2382] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-2381."  
  
[CVE-2015-2387] "ATMFD.DLL in the Adobe Type Manager Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""ATMFD.DLL Memory Corruption Vulnerability."""  
  
[CVE-2015-2416] "OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via crafted input, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""OLE Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2417."  
  
[CVE-2015-2417] "OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via crafted input, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""OLE Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2416."  
  
[CVE-2015-2423] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitive information via a crafted command-line parameter to an Office application or Notepad, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""Unsafe Command Line Parameter Passing Vulnerability."""  
  
[CVE-2015-2426] "Buffer underflow in atmfd.dll in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Driver Vulnerability."""  
  
[CVE-2015-2428] "Object Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels during interaction with object symbolic links that originated in a sandboxed process, which allows local users to gain privileges via a crafted application, aka ""Windows Object Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2429] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow attackers to bypass an application sandbox protection mechanism and perform unspecified registry actions via a crafted application, aka ""Windows Registry Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2430] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow attackers to bypass an application sandbox protection mechanism and perform unspecified filesystem actions via a crafted application, aka ""Windows Filesystem Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2432] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2433] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""Kernel ASLR Bypass Vulnerability."""  
  
[CVE-2015-2435] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Silverlight before 5.1.40728 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2015-2453] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information via a crafted application that continues to execute during a subsequent user's login session, aka ""Windows CSRSS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2454] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows KMD Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2455] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2456."  
  
[CVE-2015-2456] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2455."  
  
[CVE-2015-2458] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2459 and CVE-2015-2461."  
  
[CVE-2015-2459] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2458 and CVE-2015-2461."  
  
[CVE-2015-2460] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2461] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2458 and CVE-2015-2459."  
  
[CVE-2015-2462] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2463] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2464."  
  
[CVE-2015-2464] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2463."  
  
[CVE-2015-2465] "The Windows shell in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Shell Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2472] "Remote Desktop Session Host (RDSH) in Remote Desktop Protocol (RDP) through 8.1 in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly verify certificates, which allows man-in-the-middle attackers to spoof clients via a crafted certificate with valid Issuer and Serial Number fields, aka ""Remote Desktop Session Host Spoofing Vulnerability."""  
  
[CVE-2015-2473] "Untrusted search path vulnerability in the client in Remote Desktop Protocol (RDP) through 8.1 in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rdp file, aka ""Remote Desktop Protocol DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-2474] "Microsoft Windows Vista SP2 and Server 2008 SP2 allow remote authenticated users to execute arbitrary code via a crafted string in a Server Message Block (SMB) server error-logging action, aka ""Server Message Block Memory Corruption Vulnerability."""  
  
[CVE-2015-2475] "Cross-site scripting (XSS) vulnerability in uddi/search/frames.aspx in the UDDI Services component in Microsoft Windows Server 2008 SP2 and BizTalk Server 2010, 2013 Gold, and 2013 R2 allows remote attackers to inject arbitrary web script or HTML via the search parameter, aka ""UDDI Services Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2476] "The WebDAV client in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 supports SSL 2.0, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and conducting a decryption attack, aka ""WebDAV Client Information Disclosure Vulnerability."""  
  
[CVE-2015-2478] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application that triggers a Winsock call referencing an invalid address, aka ""Winsock Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2506] "atmfd.dll in the Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to cause a denial of service (system crash) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2507] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2512."  
  
[CVE-2015-2508] "The Adobe Type Manager Library in Microsoft Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2509] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted Media Center link (mcl) file, aka ""Windows Media Center RCE Vulnerability."""  
  
[CVE-2015-2510] "Buffer overflow in the Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""Graphics Component Buffer Overflow Vulnerability."""  
  
[CVE-2015-2511] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2517, CVE-2015-2518, and CVE-2015-2546."  
  
[CVE-2015-2512] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2507."  
  
[CVE-2015-2513] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2514 and CVE-2015-2530."  
  
[CVE-2015-2514] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2513 and CVE-2015-2530."  
  
[CVE-2015-2515] "Use-after-free vulnerability in Windows Shell in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted toolbar object, aka ""Toolbar Use After Free Vulnerability."""  
  
[CVE-2015-2516] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to cause a denial of service (data loss) via a crafted .jnt file, aka ""Windows Journal DoS Vulnerability."""  
  
[CVE-2015-2517] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2518, and CVE-2015-2546."  
  
[CVE-2015-2518] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2546."  
  
[CVE-2015-2519] "Integer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal Integer Overflow RCE Vulnerability."""  
  
[CVE-2015-2524] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Task Management Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2528."  
  
[CVE-2015-2525] "Task Scheduler in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to bypass intended filesystem restrictions and delete arbitrary files via unspecified vectors, aka ""Windows Task File Deletion Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2527] "The process-initialization implementation in win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2528] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Task Management Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2524."  
  
[CVE-2015-2529] "The kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""Kernel ASLR Bypass Vulnerability."""  
  
[CVE-2015-2530] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2513 and CVE-2015-2514."  
  
[CVE-2015-2534] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows 10 improperly processes ACL settings, which allows local users to bypass intended network-traffic restrictions via a crafted application, aka ""Hyper-V Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2535] "Active Directory in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (service outage) by creating multiple machine accounts, aka ""Active Directory Denial of Service Vulnerability."""  
  
[CVE-2015-2546] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2518."  
  
[CVE-2015-2548] "Use-after-free vulnerability in the Tablet Input Band in Windows Shell in Microsoft Windows Vista SP2 and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Microsoft Tablet Input Band Use After Free Vulnerability."""  
  
[CVE-2015-2549] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability."""  
  
[CVE-2015-2550] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2552] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows physically proximate attackers to bypass the Trusted Boot protection mechanism, and consequently interfere with the integrity of code, BitLocker, Device Encryption, and Device Health Attestation, via a crafted Boot Configuration Data (BCD) setting, aka ""Trusted Boot Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2553] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 mishandles junctions during mountpoint creation, which makes it easier for local users to gain privileges by leveraging certain sandbox access, aka ""Windows Mount Point Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2554] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Object Reference Elevation of Privilege Vulnerability."""  
  
[CVE-2015-4949] IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server 7.1 before 7.1.2, Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server 7.1 before 7.1.2, and Tivoli Storage FlashCopy Manager 4.1 before 4.1.2 place cleartext passwords in exception messages, which allows physically proximate attackers to obtain sensitive information by reading GUI pop-up windows, a different vulnerability than CVE-2015-6557.  
  
[CVE-2015-6095] "Kerberos in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles password changes, which allows physically proximate attackers to bypass authentication, and conduct decryption attacks against certain BitLocker configurations, by connecting to an unintended Key Distribution Center (KDC), aka ""Windows Kerberos Security Feature Bypass."""  
  
[CVE-2015-6097] "Heap-based buffer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted Journal (.jnt) file, aka ""Windows Journal Heap Overflow Vulnerability."""  
  
[CVE-2015-6098] "Buffer overflow in the Network Driver Interface Standard (NDIS) implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""Windows NDIS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-6100] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6101."  
  
[CVE-2015-6101] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6100."  
  
[CVE-2015-6102] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to bypass the KASLR protection mechanism, and consequently discover a driver base address, via a crafted application, aka ""Windows Kernel Memory Information Disclosure Vulnerability."""  
  
[CVE-2015-6103] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-6104."  
  
[CVE-2015-6104] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-6103."  
  
[CVE-2015-6106] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Graphics Memory Corruption Vulnerability."""  
  
[CVE-2015-6107] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10 Gold and 1511, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Graphics Memory Corruption Vulnerability."""  
  
[CVE-2015-6108] "The Windows font library in Microsoft Windows Vista SP2  
[CVE-2015-6109] "The kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the KASLR protection mechanism, and consequently discover a driver base address, via a crafted application, aka ""Windows Kernel Memory Information Disclosure Vulnerability."""  
  
[CVE-2015-6111] "IPSec in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles encryption negotiation, which allows remote authenticated users to cause a denial of service (system hang) via crafted IP traffic, aka ""Windows IPSec Denial of Service Vulnerability."""  
  
[CVE-2015-6112] "SChannel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 lacks the required extended master-secret binding support to ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers to obtain sensitive information or modify TLS session data via a ""triple handshake attack,"" aka ""Schannel TLS Triple Handshake Vulnerability."""  
  
[CVE-2015-6113] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to bypass intended filesystem permissions by leveraging Low Integrity access, aka ""Windows Kernel Security Feature Bypass Vulnerability."""  
  
[CVE-2015-6125] "Use-after-free vulnerability in the DNS server in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka ""Windows DNS Use After Free Vulnerability."""  
  
[CVE-2015-6126] "Race condition in the Pragmatic General Multicast (PGM) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application, aka ""Windows PGM UAF Elevation of Privilege Vulnerability."""  
  
[CVE-2015-6127] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows remote attackers to read arbitrary files via a crafted .mcl file, aka ""Windows Media Center Information Disclosure Vulnerability."""  
  
[CVE-2015-6128] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6130] "Integer underflow in Uniscribe in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows remote attackers to execute arbitrary code via a crafted font, aka ""Windows Integer Underflow Vulnerability."""  
  
[CVE-2015-6131] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted .mcl file, aka ""Media Center Library Parsing RCE Vulnerability."""  
  
[CVE-2015-6132] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6133] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6171] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6173 and CVE-2015-6174."  
  
[CVE-2015-6173] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6171 and CVE-2015-6174."  
  
[CVE-2015-6174] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6171 and CVE-2015-6173."  
  
[CVE-2015-6175] "The kernel in Microsoft Windows 10 Gold allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0006] "The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka ""Windows Mount Point Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0007."  
  
[CVE-2016-0007] "The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka ""Windows Mount Point Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0006."  
  
[CVE-2016-0008] "The graphics device interface in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka ""Windows GDI32.dll ASLR Bypass Vulnerability."""  
  
[CVE-2016-0009] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via unspecified vectors, aka ""Win32k Remote Code Execution Vulnerability."""  
  
[CVE-2016-0014] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0015] "DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""DirectShow Heap Corruption Remote Code Execution Vulnerability."""  
  
[CVE-2016-0016] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0018] "Microsoft Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 R2, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0019] "The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka ""Windows Remote Desktop Protocol Security Bypass Vulnerability."""  
  
[CVE-2016-0020] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""MAPI DLL Loading Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0026] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-0036] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote authenticated users to execute arbitrary code via crafted data, aka ""Remote Desktop Protocol (RDP) Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0037] "The forms-based authentication implementation in Active Directory Federation Services (ADFS) 3.0 in Microsoft Windows Server 2012 R2 allows remote attackers to cause a denial of service (daemon outage) via crafted data, aka ""Microsoft Active Directory Federation Services Denial of Service Vulnerability."""  
  
[CVE-2016-0038] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Memory Corruption Vulnerability."""  
  
[CVE-2016-0040] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0041] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 10 and 11 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0042] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""Windows DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0044] "Sync Framework in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows remote attackers to cause a denial of service (SyncShareSvc service outage) via crafted ""change batch"" data, aka ""Windows DLL Loading Denial of Service Vulnerability."""  
  
[CVE-2016-0046] "Windows Reader in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted Reader file, aka ""Microsoft Windows Reader Vulnerability."""  
  
[CVE-2016-0047] "WinForms in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 allows remote attackers to obtain sensitive information from process memory via crafted icon data, aka ""Windows Forms Information Disclosure Vulnerability."""  
  
[CVE-2016-0048] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0049] "Kerberos in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 does not properly validate password changes, which allows remote attackers to bypass authentication by deploying a crafted Key Distribution Center (KDC) and then performing a sign-in action, aka ""Windows Kerberos Security Feature Bypass."""  
  
[CVE-2016-0050] "Network Policy Server (NPS) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 misparses username queries, which allows remote attackers to cause a denial of service (RADIUS authentication outage) via crafted requests, aka ""Network Policy Server RADIUS Implementation Denial of Service Vulnerability."""  
  
[CVE-2016-0051] "The WebDAV client in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""WebDAV Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0058] "Buffer overflow in the PDF Library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted PDF document that triggers API calls, aka ""Microsoft PDF Library Buffer Overflow Vulnerability."""  
  
[CVE-2016-0070] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0073] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0075."  
  
[CVE-2016-0075] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0073."  
  
[CVE-2016-0079] "The kernel in Microsoft Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0087] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 do not properly validate handles, which allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0088] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows guest OS users to execute arbitrary code on the host OS via a crafted application, aka ""Hyper-V Remote Code Execution Vulnerability."""  
  
[CVE-2016-0089] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows guest OS users to obtain sensitive information from host OS memory via a crafted application, aka ""Hyper-V Information Disclosure Vulnerability."""  
  
[CVE-2016-0090] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows 10 allows guest OS users to obtain sensitive information from host OS memory via a crafted application, aka ""Hyper-V Information Disclosure Vulnerability."""  
  
[CVE-2016-0091] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2016-0092."  
  
[CVE-2016-0092] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2016-0091."  
  
[CVE-2016-0093] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0094, CVE-2016-0095, and CVE-2016-0096."  
  
[CVE-2016-0094] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0095, and CVE-2016-0096."  
  
[CVE-2016-0095] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0096."  
  
[CVE-2016-0096] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0095."  
  
[CVE-2016-0098] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 allow remote attackers to execute arbitrary code via crafted media content, aka ""Windows Media Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2016-0099] "The Secondary Logon Service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 does not properly process request handles, which allows local users to gain privileges via a crafted application, aka ""Secondary Logon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0100] "Microsoft Windows Vista SP2 and Server 2008 SP2 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Library Loading Input Validation Remote Code Execution Vulnerability."""  
  
[CVE-2016-0101] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via crafted media content, aka ""Windows Media Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2016-0117] "The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-0118] "The PDF library in Microsoft Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-0120] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2016-0121] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2016-0133] "The USB Mass Storage Class driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows physically proximate attackers to execute arbitrary code by inserting a crafted USB device, aka ""USB Mass Storage Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0135] "The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Secondary Logon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0142] "Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted web page, aka ""Microsoft Video Control Remote Code Execution Vulnerability."""  
  
[CVE-2016-0143] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0165 and CVE-2016-0167."  
  
[CVE-2016-0145] "The font library in Microsoft Windows Vista SP2  
[CVE-2016-0150] "HTTP.sys in Microsoft Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via crafted HTTP 2.0 requests, aka ""HTTP.sys Denial of Service Vulnerability."""  
  
[CVE-2016-0151] "The Client-Server Run-time Subsystem (CSRSS) in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mismanages process tokens, which allows local users to gain privileges via a crafted application, aka ""Windows CSRSS Security Feature Bypass Vulnerability."""  
  
[CVE-2016-0152] "Internet Information Services (IIS) in Microsoft Windows Vista SP2 and Server 2008 SP2 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0153] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Remote Code Execution Vulnerability."""  
  
[CVE-2016-0165] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0143 and CVE-2016-0167."  
  
[CVE-2016-0167] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0143 and CVE-2016-0165."  
  
[CVE-2016-0168] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to obtain sensitive information via a crafted document, aka ""Windows Graphics Component Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-0169."  
  
[CVE-2016-0169] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to obtain sensitive information via a crafted document, aka ""Windows Graphics Component Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-0168."  
  
[CVE-2016-0170] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Windows Graphics Component RCE Vulnerability."""  
  
[CVE-2016-0171] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0173, CVE-2016-0174, and CVE-2016-0196."  
  
[CVE-2016-0173] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0174, and CVE-2016-0196."  
  
[CVE-2016-0174] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0196."  
  
[CVE-2016-0175] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to obtain sensitive information about kernel-object addresses, and consequently bypass the KASLR protection mechanism, via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-0176] "dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0179] "Windows Shell in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Shell Remote Code Execution Vulnerability."""  
  
[CVE-2016-0180] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles symbolic links, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0181] "Microsoft Windows 10 Gold and 1511 allows local users to bypass the Virtual Secure Mode Hypervisor Code Integrity (HVCI) protection mechanism and perform RWX markings of kernel-mode pages via a crafted application, aka ""Hypervisor Code Integrity Security Feature Bypass."""  
  
[CVE-2016-0182] "Windows Journal in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal (aka .jnt) file, aka ""Windows Journal Memory Corruption Vulnerability."""  
  
[CVE-2016-0183] "The Windows font library in Microsoft Office 2010 SP2, Word 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Microsoft Office Graphics RCE Vulnerability."""  
  
[CVE-2016-0184] "Use-after-free vulnerability in GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Direct3D Use After Free Vulnerability."""  
  
[CVE-2016-0185] "Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted Media Center link (aka .mcl) file, aka ""Windows Media Center Remote Code Execution Vulnerability."""  
  
[CVE-2016-0190] "Volume Manager Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 does not properly check whether RemoteFX RDP USB disk accesses originate from the user who mounted a disk, which allows local users to read arbitrary files on these disks via RemoteFX requests, aka ""Remote Desktop Protocol Drive Redirection Information Disclosure Vulnerability."""  
  
[CVE-2016-0195] "The Imaging Component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Windows Imaging Component Memory Corruption Vulnerability."""  
  
[CVE-2016-0196] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0174."  
  
[CVE-2016-0197] "dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3201] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka ""Windows PDF Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3215."  
  
[CVE-2016-3203] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows PDF Remote Code Execution Vulnerability."""  
  
[CVE-2016-3209] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3213] "The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 9 through 11 has an improper fallback mechanism, which allows remote attackers to gain privileges via NetBIOS name responses, aka ""WPAD Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3215] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka ""Windows PDF Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3201."  
  
[CVE-2016-3216] "GDI32.dll in the Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka ""Windows Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2016-3218] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3221."  
  
[CVE-2016-3219] "The kernel-mode driver in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3220] "atmfd.dll in the Adobe Type Manager Font Driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""ATMFD.dll Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3221] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3218."  
  
[CVE-2016-3223] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandle LDAP authentication, which allows man-in-the-middle attackers to gain privileges by modifying group-policy update data within a domain-controller data stream, aka ""Group Policy Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3225] "The SMB server component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application that forwards an authentication request to an unintended service, aka ""Windows SMB Server Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3226] "Active Directory in Microsoft Windows Server 2008 R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (service hang) by creating many machine accounts, aka ""Active Directory Denial of Service Vulnerability."""  
  
[CVE-2016-3227] "Use-after-free vulnerability in the DNS Server component in Microsoft Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka ""Windows DNS Server Use After Free Vulnerability."""  
  
[CVE-2016-3228] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Windows Server 2012 Gold and R2 allow remote authenticated users to execute arbitrary code via a crafted NetLogon request, aka ""Windows Netlogon Memory Corruption Remote Code Execution Vulnerability."""  
  
[CVE-2016-3230] "The Search component in Microsoft Windows 7, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to cause a denial of service (performance degradation) via a crafted application, aka ""Windows Search Component Denial of Service Vulnerability."""  
  
[CVE-2016-3232] "The Virtual PCI (VPCI) virtual service provider in Microsoft Windows Server 2012 Gold and R2 allows local users to obtain sensitive information from uninitialized memory locations via a crafted application, aka ""Windows Virtual PCI Information Disclosure Vulnerability."""  
  
[CVE-2016-3236] "The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka ""Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3237] "Kerberos in Microsoft Windows Vista SP2  
[CVE-2016-3238] "The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows man-in-the-middle attackers to execute arbitrary code by providing a crafted print driver during printer installation, aka ""Windows Print Spooler Remote Code Execution Vulnerability."""  
  
[CVE-2016-3239] "The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via vectors involving filesystem write operations, aka ""Windows Print Spooler Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3249] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3252, CVE-2016-3254, and CVE-2016-3286."  
  
[CVE-2016-3250] "The kernel-mode drivers in Microsoft Windows Server 2012 and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3251] "The GDI component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to obtain sensitive kernel-address information via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-3252] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3254, and CVE-2016-3286."  
  
[CVE-2016-3254] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3286."  
  
[CVE-2016-3256] "Microsoft Windows 10 Gold and 1511 allows local users to bypass the Secure Kernel Mode protection mechanism and obtain sensitive information via a crafted application, aka ""Windows Secure Kernel Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-3258] "Race condition in the kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Low Integrity protection mechanism and write to files by leveraging unspecified object-manager features, aka ""Windows File System Security Feature Bypass."""  
  
[CVE-2016-3262] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3263] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3266] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3376, CVE-2016-7185, and CVE-2016-7211."  
  
[CVE-2016-3270] "The Graphics component in the kernel in Microsoft Windows Vista SP2  
[CVE-2016-3272] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles page-fault system calls, which allows local users to obtain sensitive information from an arbitrary process via a crafted application, aka ""Windows Kernel Information Disclosure Vulnerability."""  
  
[CVE-2016-3286] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3254."  
  
[CVE-2016-3287] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Secure Boot protection mechanism by leveraging administrative access to install a crafted policy, aka ""Secure Boot Security Feature Bypass."""  
  
[CVE-2016-3298] "Microsoft Internet Explorer 9 through 11 and the Internet Messaging API in Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to determine the existence of arbitrary files via a crafted web site, aka ""Internet Explorer Information Disclosure Vulnerability."""  
  
[CVE-2016-3299] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to hijack network traffic or bypass intended Enhanced Protected Mode (EPM) or application container protection mechanisms, and consequently render untrusted content in a browser, by leveraging how NetBIOS validates responses, aka ""NetBIOS Spoofing Vulnerability."""  
  
[CVE-2016-3300] "The Netlogon service in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 improperly establishes secure communications channels, which allows local users to gain privileges by leveraging access to a domain-joined machine, aka ""Netlogon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3301] "The Windows font library in Microsoft Windows Vista SP2  
[CVE-2016-3302] "Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607, when the lock screen is enabled, do not properly restrict the loading of web content, which allows physically proximate attackers to execute arbitrary code via a (1) crafted Wi-Fi access point or (2) crafted mobile-broadband device, aka ""Windows Lock Screen Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3303] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Component RCE Vulnerability,"" a different vulnerability than CVE-2016-3304."  
  
[CVE-2016-3304] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Component RCE Vulnerability,"" a different vulnerability than CVE-2016-3303."  
  
[CVE-2016-3305] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka ""Windows Session Object Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3306."  
  
[CVE-2016-3306] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka ""Windows Session Object Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3305."  
  
[CVE-2016-3308] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3309] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3310] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3311] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3312] "ActiveSyncProvider in Microsoft Windows 10 Gold and 1511 allows attackers to discover credentials by leveraging failure of Universal Outlook to obtain a secure connection, aka ""Universal Outlook Information Disclosure Vulnerability."""  
  
[CVE-2016-3319] "The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allows remote attackers to execute arbitrary code via a crafted PDF file, aka ""Microsoft PDF Remote Code Execution Vulnerability."""  
  
[CVE-2016-3320] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow attackers to bypass the Secure Boot protection mechanism by leveraging (1) administrative or (2) physical access to install a crafted boot manager, aka ""Secure Boot Security Feature Bypass."""  
  
[CVE-2016-3332] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3333] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3334] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3335] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3338] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3340] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3341] "The kernel-mode drivers in Transaction Manager in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Windows Transaction Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3342] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3343] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-7184."  
  
[CVE-2016-3344] "The Secure Kernel Mode feature in Microsoft Windows 10 Gold and 1511 allows local users to obtain sensitive information via a crafted application, aka ""Windows Secure Kernel Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-3345] "The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via crafted packets, aka ""Windows SMB Authenticated Remote Code Execution Vulnerability."""  
  
[CVE-2016-3346] "Microsoft Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain Administrator access via a crafted DLL, aka ""Windows Permissions Enforcement Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3348] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3349] "The kernel-mode drivers in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3352] "Microsoft Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 do not properly check NTLM SSO requests for MSA logins, which makes it easier for remote attackers to determine passwords via a brute-force attack on NTLM password hashes, aka ""Microsoft Information Disclosure Vulnerability."""  
  
[CVE-2016-3354] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2016-3355] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka ""GDI Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3356] "The Graphics Device Interface (GDI) in Microsoft Windows 10 1607 allows remote attackers to execute arbitrary code via a crafted document, aka ""GDI Remote Code Execution Vulnerability."""  
  
[CVE-2016-3368] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote authenticated users to execute arbitrary code by leveraging a domain account to make a crafted request, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-3369] "Microsoft Windows 10 Gold and 1511 allows attackers to cause a denial of service via unspecified vectors, aka ""Windows Denial of Service Vulnerability."""  
  
[CVE-2016-3370] "The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka ""PDF Library Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3374."  
  
[CVE-2016-3371] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain sensitive information via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3372] "The kernel API in Microsoft Windows Vista SP2 and Windows Server 2008 SP2 does not properly enforce permissions, which allows local users to spoof processes, spoof inter-process communication, or cause a denial of service via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3373] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly implement registry access control, which allows local users to obtain sensitive account information via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3374] "The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka ""PDF Library Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3370."  
  
[CVE-2016-3375] "The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Scripting Engine Memory Corruption Vulnerability."""  
  
[CVE-2016-3376] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-7185, and CVE-2016-7211."  
  
[CVE-2016-3393] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3396] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-5063] The RSCD agent in BMC Server Automation before 8.6 SP1 Patch 2 and 8.7 before Patch 3 on Windows might allow remote attackers to bypass authorization checks and make an RPC call via unspecified vectors.  
  
[CVE-2016-6848] "An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. API requests can be used to inject, generate and download executable files to the client (""Reflected File Download""). Malicious platform specific (e.g. Microsoft Windows) batch file can be created via a trusted domain without authentication that, if executed by the user, may lead to local code execution."  
  
[CVE-2016-7165] "A vulnerability has been identified in Primary Setup Tool (PST) (All versions < V4.2 HF1), SIMATIC IT Production Suite (All versions < V7.0 SP1 HFX 2), SIMATIC NET PC-Software (All versions < V14), SIMATIC PCS 7 V7.1 (All versions), SIMATIC PCS 7 V8.0 (All versions), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions < V8.2 SP1), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2), SIMATIC STEP 7 V5.X (All versions < V5.5 SP4 HF11), SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced (All versions < V14), SIMATIC WinCC (TIA Portal) Professional V13 (All versions < V13 SP2), SIMATIC WinCC (TIA Portal) Professional V14 (All versions < V14 SP1), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2), SIMATIC WinCC Runtime Professional V14 (All versions < V14 SP1), SIMATIC WinCC V7.0 SP2 and earlier versions (All versions < V7.0 SP2 Upd 12), SIMATIC WinCC V7.0 SP3 (All versions < V7.0 SP3 Upd 8), SIMATIC WinCC V7.2 (All versions < V7.2 Upd 14), SIMATIC WinCC V7.3 (All versions < V7.3 Upd 11), SIMATIC WinCC V7.4 (All versions < V7.4 SP1), SIMIT V9.0 (All versions < V9.0 SP1), SINEMA Remote Connect Client (All versions < V1.0 SP3), SINEMA Server (All versions < V13 SP2), SOFTNET Security Client V5.0 (All versions), Security Configuration Tool (SCT) (All versions < V4.3 HF1), TeleControl Server Basic (All versions < V3.0 SP2), WinAC RTX 2010 SP2 (All versions), WinAC RTX F 2010 SP2 (All versions). Unquoted service paths could allow local Microsoft Windows operating system users to escalate their privileges if the affected products are not installed under their default path (""C:\Program Files\\*"" or the localized equivalent)."  
  
[CVE-2016-7182] "The Graphics component in Microsoft Windows Vista SP2  
[CVE-2016-7184] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-3343."  
  
[CVE-2016-7185] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7211."  
  
[CVE-2016-7188] "The Standard Collector Service in Windows Diagnostics Hub in Microsoft Windows 10 Gold, 1511, and 1607 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Diagnostics Hub Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7205] "Animation Manager in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Animation Manager Memory Corruption Vulnerability."""  
  
[CVE-2016-7210] "atmfd.dll in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted Open Type font on a web site, aka ""Open Type Font Information Disclosure Vulnerability."""  
  
[CVE-2016-7211] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7185."  
  
[CVE-2016-7212] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow remote attackers to execute arbitrary code via a crafted image file, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-7214] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to bypass the ASLR protection mechanism via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-7215] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7216] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandles permissions, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7217] "Media Foundation in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Media Foundation Memory Corruption Vulnerability."""  
  
[CVE-2016-7218] "Bowser.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Windows Bowser.sys Information Disclosure Vulnerability."""  
  
[CVE-2016-7219] "The Crypto driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Windows Crypto Driver Information Disclosure Vulnerability."""  
  
[CVE-2016-7220] "Virtual Secure Mode in Microsoft Windows 10 allows local users to obtain sensitive information via a crafted application, aka ""Virtual Secure Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-7221] "Input Method Editor (IME) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles DLL loading, which allows local users to gain privileges via unspecified vectors, aka ""Windows IME Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7222] "Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a crafted UNC pathname in a task, aka ""Task Scheduler Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7223] "Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka ""VHD Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7224] "Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka ""VHD Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7237] "Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote authenticated users to cause a denial of service (system hang) via a crafted request, aka ""Local Security Authority Subsystem Service Denial of Service Vulnerability."""  
  
[CVE-2016-7238] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandle caching for NTLM password-change requests, which allows local users to gain privileges via a crafted application, aka ""Windows NTLM Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7246] "The kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7247] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow physically proximate attackers to bypass the Secure Boot protection mechanism via a crafted boot policy, aka ""Secure Boot Component Vulnerability."""  
  
[CVE-2016-7248] "Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka ""Microsoft Video Control Remote Code Execution Vulnerability."""  
  
[CVE-2016-7255] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7256] "atmfd.dll in the Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Open Type Font Remote Code Execution Vulnerability."""  
  
[CVE-2016-7257] "The GDI component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office for Mac 2011, and Office 2016 for Mac allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2016-7258] "The kernel in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 mishandles page-fault system calls, which allows local users to obtain sensitive information from arbitrary processes via a crafted application, aka ""Windows Kernel Memory Address Information Disclosure Vulnerability."""  
  
[CVE-2016-7259] "The Graphics Component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7260] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7271] "The Secure Kernel Mode implementation in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to bypass the virtual trust level (VTL) protection mechanism via a crafted application, aka ""Secure Kernel Mode Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7272] "The Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Graphics Remote Code Execution Vulnerability."""  
  
[CVE-2016-7273] "The Graphics component in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Graphics Remote Code Execution Vulnerability."""  
  
[CVE-2016-7274] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."""  
  
[CVE-2016-7278] "Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Windows Hyperlink Object Library Information Disclosure Vulnerability."""  
  
[CVE-2016-7292] "The Installer in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Installer Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7295] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information from process memory via a crafted application, aka ""Windows Common Log File System Driver Information Disclosure Vulnerability."""  
  
[CVE-2016-9192] A vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and execute an arbitrary executable file with privileges equivalent to the Microsoft Windows operating system SYSTEM account. More Information: CSCvb68043. Known Affected Releases: 4.3(2039) 4.3(748). Known Fixed Releases: 4.3(4019) 4.4(225).  
  
[CVE-2016-9459] Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a log pollution vulnerability potentially leading to a local XSS. The download log functionality in the admin screen is delivering the log in JSON format to the end-user. The file was delivered with an attachment disposition forcing the browser to download the document. However, Firefox running on Microsoft Windows would offer the user to open the data in the browser as an HTML document. Thus any injected data in the log would be executed.  
  
[CVE-2017-0001] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0004] "The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to cause a denial of service (reboot) via a crafted authentication request, aka ""Local Security Authority Subsystem Service Denial of Service Vulnerability."""  
  
[CVE-2017-0005] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0007] "Device Guard in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows remote attackers to modify PowerShell script without invalidating associated signatures, aka ""PowerShell Security Feature Bypass Vulnerability."""  
  
[CVE-2017-0014] "The Windows Graphics Component in Microsoft Office 2010 SP2  
[CVE-2017-0016] "Microsoft Windows 10 Gold, 1511, and 1607  
[CVE-2017-0021] "Hyper-V in Microsoft Windows 10 1607 and Windows Server 2016 does not properly validate vSMB packet data, which allows attackers to execute arbitrary code on a target OS, aka ""Hyper-V System Data Structure Vulnerability."" This vulnerability is different from that described in CVE-2017-0095."  
  
[CVE-2017-0022] "Microsoft XML Core Services (MSXML) in Windows 10 Gold, 1511, and 1607  
[CVE-2017-0024] "The kernel-mode drivers in Microsoft Windows 10 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0025] "The kernel-mode drivers in Microsoft Windows Vista  
[CVE-2017-0026] "The kernel-mode drivers in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0038] gdi32.dll in Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information from process heap memory via a crafted EMF file, as demonstrated by an EMR\_SETDIBITSTODEVICE record with modified Device Independent Bitmap (DIB) dimensions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-3216, CVE-2016-3219, and/or CVE-2016-3220.  
  
[CVE-2017-0039] "Microsoft Windows Vista SP2 and Server 2008 SP2 mishandle dynamic link library (DLL) loading, which allows local users to gain privileges via a crafted application, aka ""Library Loading Input Validation Remote Code Execution Vulnerability."""  
  
[CVE-2017-0042] "Windows Media Player in Microsoft Windows 8.1  
[CVE-2017-0043] "Active Directory Federation Services in Microsoft Windows 10 1607, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Microsoft Active Directory Federation Services Information Disclosure Vulnerability."""  
  
[CVE-2017-0047] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0050] "The kernel API in Microsoft Windows Vista SP2  
[CVE-2017-0051] "Microsoft Windows 10 1607 and Windows Server 2016 allow remote attackers to cause a denial of service (application hang) via a crafted Office document, aka ""Microsoft Hyper-V Network Switch Denial of Service Vulnerability."" This vulnerability is different from those described in CVE-2017-0074, CVE-2017-0076, CVE-2017-0097, CVE-2017-0098, and CVE-2017-0099."  
  
[CVE-2017-0055] "Microsoft Internet Information Server (IIS) in Windows Vista SP2  
[CVE-2017-0056] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2017-0057] "DNS client in Microsoft Windows 8.1  
[CVE-2017-0058] "A Win32k information disclosure vulnerability exists in Microsoft Windows when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2017-0060] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0061] "The Color Management Module (ICM32.dll) memory handling functionality in Windows Vista SP2, Windows Server 2008 SP2 and R2, and Windows 7 SP1 allows remote attackers to bypass ASLR and execute code in combination with another vulnerability through a crafted website, aka ""Microsoft Color Management Information Disclosure Vulnerability."" This vulnerability is different from that described in CVE-2017-0063."  
  
[CVE-2017-0062] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0066] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0135 and CVE-2017-0140."  
  
[CVE-2017-0072] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0073] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0074] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0075] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0076] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0078] "The kernel-mode drivers in Microsoft Windows 8.1  
[CVE-2017-0080] "The kernel-mode drivers in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0081] "The kernel-mode drivers in Microsoft Windows 8.1  
[CVE-2017-0082] "The kernel-mode drivers in Microsoft Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, and CVE-2017-0081."  
  
[CVE-2017-0083] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0084] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0085] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0086] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0087] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0088] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."""  
  
[CVE-2017-0089] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0090."  
  
[CVE-2017-0090] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0089."  
  
[CVE-2017-0091] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0092] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0095] "Hyper-V in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 does not properly validate vSMB packet data, which allows attackers to execute arbitrary code on a target OS, aka ""Hyper-V vSMB Remote Code Execution Vulnerability."" This vulnerability is different from that described in CVE-2017-0021."  
  
[CVE-2017-0096] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0097] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0098] "Hyper-V in Microsoft Windows 10 Gold, 1511, and 1607  
[CVE-2017-0099] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0100] "A DCOM object in Helppane.exe in Microsoft Windows 7 SP1  
[CVE-2017-0101] "The kernel-mode drivers in Transaction Manager in Microsoft Windows Vista SP2  
[CVE-2017-0102] "Microsoft Windows Vista SP2  
[CVE-2017-0103] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows Server 2012 mishandles registry objects in memory, which allows local users to gain privileges via a crafted application, aka ""Windows Registry Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0104] "The iSNS Server service in Microsoft Windows Server 2008 SP2 and R2, Windows Server 2012 Gold and R2, and Windows Server 2016 allows remote attackers to issue malicious requests via an integer overflow, aka ""iSNS Server Memory Corruption Vulnerability."""  
  
[CVE-2017-0108] "The Windows Graphics Component in Microsoft Office 2007 SP3  
[CVE-2017-0109] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0111] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0112] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0113] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0114] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0115] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0116] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0117] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0118] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0119] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0120] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Windows Uniscribe Information Disclosure Vulnerability."""  
  
[CVE-2017-0121] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0122] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0123] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0124] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0125] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0126] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0127] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, and CVE-2017-0128."  
  
[CVE-2017-0128] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, and CVE-2017-0127."  
  
[CVE-2017-0135] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0140."  
  
[CVE-2017-0140] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0135."  
  
[CVE-2017-0143] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0144] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0145] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0146] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0147] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0148] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0154] "Microsoft Internet Explorer 11 on Windows 10, 1511, and 1606 and Windows Server 2016 does not enforce cross-domain policies, allowing attackers to access information from one domain and inject it into another via a crafted application, aka, ""Internet Explorer Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0155] "The Graphics component in the kernel in Microsoft Windows Vista SP2  
[CVE-2017-0156] "An elevation of privilege vulnerability exists in Windows 7, Windows 8.1, Windows RT 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 when the Microsoft Graphics Component fails to properly handle objects in memory, aka ""Windows Graphics Component Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0158] "An elevation of privilege vulnerability exists when Microsoft Windows running on Windows 10, Windows 10 1511, Windows 8.1 Windows RT 8.1, and Windows Server 2012 R2 fails to properly sanitize handles in memory, aka ""Scripting Engine Memory Corruption Vulnerability."""  
  
[CVE-2017-0161] "The Windows NetBT Session Services component on Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to maintain certain sequencing requirements, aka ""NetBIOS Remote Code Execution Vulnerability""."  
  
[CVE-2017-0165] "An elevation of privilege vulnerability exists when Microsoft Windows running on Windows 10, Windows 10 1511, Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 fails to properly sanitize handles in memory, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0171] "Windows DNS Server allows a denial of service vulnerability when Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 are configured to answer version queries, aka ""Windows DNS Server Denial of Service Vulnerability""."  
  
[CVE-2017-0173] "Microsoft Windows 10 1607 and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0215, CVE-2017-0216, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0176] A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.  
  
[CVE-2017-0178] "A denial of service vulnerability exists when Microsoft Hyper-V running on Windows 10, Windows 10 1511, Windows 10 1607, Windows 8.1, Windows Server 2012 R2, and Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0179] "A denial of service vulnerability exists when Microsoft Hyper-V running on a Windows 10, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0182] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0183] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0185] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, and CVE-2017-0186."  
  
[CVE-2017-0186] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, and CVE-2017-0185."  
  
[CVE-2017-0190] "The GDI component in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2017-0192] "The Adobe Type Manager Font Driver (ATMFD.dll) in Microsoft Windows Vista SP2  
[CVE-2017-0193] "Windows Hyper-V in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to gain elevated privileges on a target guest operating system when Windows Hyper-V instruction emulation fails to properly enforce privilege levels, aka ""Hypervisor Code Integrity Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0199] "Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka ""Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."""  
  
[CVE-2017-0211] "An elevation of privilege vulnerability exists in Windows 10, Windows 8.1, Windows RT 8.1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 versions of Microsoft Windows OLE when it fails an integrity-level check, aka ""Windows OLE Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0212] "Windows Hyper-V allows an elevation of privilege vulnerability when Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 fail to properly validate vSMB packet data, aka ""Windows Hyper-V vSMB Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0213] "Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka ""Windows COM Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-0214."  
  
[CVE-2017-0214] "Windows COM in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when Windows fails to properly validate input before loading type libraries, aka ""Windows COM Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-0213."  
  
[CVE-2017-0215] "Microsoft Windows 10 1607 and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0216, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0216] "Microsoft Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0218] "Microsoft Windows 10 Gold, Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0216, and CVE-2017-0219."  
  
[CVE-2017-0219] "Microsoft Windows 10 Gold, Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0216, and CVE-2017-0218."  
  
[CVE-2017-0250] "Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to buffer overflow, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-0258] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-0175, CVE-2017-0220, and CVE-2017-0259."  
  
[CVE-2017-0259] "The Windows kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-0175, CVE-2017-0220, and CVE-2017-0258."  
  
[CVE-2017-0263] "The kernel-mode drivers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0267] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0268] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0269] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0273 and CVE-2017-0280."  
  
[CVE-2017-0270] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0271] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0272] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0277, CVE-2017-0278, and CVE-2017-0279."  
  
[CVE-2017-0273] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0269 and CVE-2017-0280."  
  
[CVE-2017-0274] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0275] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, and CVE-2017-0276."  
  
[CVE-2017-0276] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, and CVE-2017-0275."  
  
[CVE-2017-0277] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0278, and CVE-2017-0279."  
  
[CVE-2017-0278] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0277, and CVE-2017-0279."  
  
[CVE-2017-0279] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0277, and CVE-2017-0278."  
  
[CVE-2017-0280] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0269 and CVE-2017-0273."  
  
[CVE-2017-0282] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0284, CVE-2017-0285, and CVE-2017-8534."  
  
[CVE-2017-0283] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office Word Viewer, Microsoft Lync 2013 SP1, Skype for Business 2016, Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows, and Microsoft Silverlight 5 when installed on Microsoft Windows allows a remote code execution vulnerability due to the way it handles objects in memory, aka ""Windows Uniscribe Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8528."  
  
[CVE-2017-0284] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0285, and CVE-2017-8534."  
  
[CVE-2017-0285] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, and Microsoft Office Word Viewer allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0284, and CVE-2017-8534."  
  
[CVE-2017-0290] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 does not properly scan a specially crafted file leading to memory corruption, aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability."""  
  
[CVE-2017-0293] "Microsoft Windows PDF Library in Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability when it improperly handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability""."  
  
[CVE-2017-0294] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute remote code when Windows fails to properly handle cabinet files, aka ""Windows Remote Code Execution Vulnerability""."  
  
[CVE-2017-0295] "Microsoft Windows 10 1607 and 1703, and Windows Server 2016 allow an authenticated attacker to modify the C:\Users\DEFAULT folder structure, aka ""Windows Default Folder Tampering Vulnerability""."  
  
[CVE-2017-0296] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to elevate privilege when tdx.sys fails to check the length of a buffer prior to copying memory to it, aka ""Windows TDX Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0297] "The kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0299, CVE-2017-0300."  
  
[CVE-2017-0298] "A DCOM object in Helppane.exe in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016, when configured to run as the interactive user, allows an authenticated attacker to run arbitrary code in another user's session, aka ""Windows COM Session Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0299] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, and CVE-2017-0297."  
  
[CVE-2017-0300] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-10769] "XnView Classic for Windows Version 2.40 might allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .rle file, related to ""Data from Faulting Address controls Branch Selection starting at ntdll\_77df0000!memcmp+0x0000000000000018"" (without RPC initialization)."  
  
[CVE-2017-10772] "XnView Classic for Windows Version 2.40 might allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .rle file, related to ""Data from Faulting Address controls Branch Selection starting at ntdll\_77df0000!memcmp+0x0000000000000018"" (with RPC initialization)."  
  
[CVE-2017-11762] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-11763."  
  
[CVE-2017-11763] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-11763."  
  
[CVE-2017-11764] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-8756."  
  
[CVE-2017-11765] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11784, CVE-2017-11785, and CVE-2017-11814."  
  
[CVE-2017-11766] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-8751."  
  
[CVE-2017-11769] "The Microsoft Windows TRIE component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles loading dll files, aka ""TRIE Remote Code Execution Vulnerability""."  
  
[CVE-2017-11771] "The Microsoft Windows Search component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly handle DNS responses, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-11772] "The Microsoft Windows Search component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure when it fails to properly handle objects in memory, aka ""Microsoft Search Information Disclosure Vulnerability""."  
  
[CVE-2017-11779] "The Microsoft Windows Domain Name System (DNS) DNSAPI.dll on Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly handle DNS responses, aka ""Windows DNSAPI Remote Code Execution Vulnerability""."  
  
[CVE-2017-11780] "The Server Message Block 1.0 (SMBv1) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a remote code execution vulnerability when it fails to properly handle certain requests, aka ""Windows SMB Remote Code Execution Vulnerability""."  
  
[CVE-2017-11781] "The Microsoft Server Block Message (SMB) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a denial of service vulnerability when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability""."  
  
[CVE-2017-11782] "The Microsoft Server Block Message (SMB) on Microsoft Windows 10 1607 and Windows Server 2016, allows an elevation of privilege vulnerability when an attacker sends specially crafted requests to the server, aka ""Windows SMB Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11783] "Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability in the way it handles calls to Advanced Local Procedure Call (ALPC), aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11784] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11785, and CVE-2017-11814."  
  
[CVE-2017-11785] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11784, and CVE-2017-11814."  
  
[CVE-2017-11790] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2017-11791] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11834."  
  
[CVE-2017-11792] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allow an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11793, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11793] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11794] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8726 and CVE-2017-11803."  
  
[CVE-2017-11796] "ChakraCore and Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11798] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11799] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11800] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11802] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11803] "Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11833 and CVE-2017-11844."  
  
[CVE-2017-11804] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11805] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11806] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11807] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11808] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11809] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11810] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11811] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11812] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11813] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11822."  
  
[CVE-2017-11814] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11784, and CVE-2017-11785."  
  
[CVE-2017-11815] "The Microsoft Server Block Message (SMB) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability in the way that it handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability""."  
  
[CVE-2017-11816] "The Microsoft Windows Graphics Device Interface (GDI) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability in the way it handles objects in memory, aka ""Windows GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-11817] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly validates objects in memory, aka ""Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-11818] "The Microsoft Windows Storage component on Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass vulnerability when it fails to validate an integrity-level check, aka ""Windows Storage Security Feature Bypass Vulnerability""."  
  
[CVE-2017-11819] "Microsoft Windows 7 SP1 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft browsers handle objects in memory, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2017-11821] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, and CVE-2017-11812."  
  
[CVE-2017-11822] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11813."  
  
[CVE-2017-11823] "The Microsoft Device Guard on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass by the way it handles Windows PowerShell sessions, aka ""Microsoft Windows Security Feature Bypass""."  
  
[CVE-2017-11824] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability in the way it handles objects in memory, aka ""Windows Graphics Component Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11827] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability""."  
  
[CVE-2017-11829] Microsoft Windows 10 allows an elevation of privilege vulnerability when the Windows Update Delivery Optimization does not properly enforce file share permissions.  
  
[CVE-2017-11832] "The Microsoft Windows embedded OpenType (EOT) font engine in Windows 7 SP1, Windows Server 2008 SP2 and 2008 R2 SP1, and Windows Server 2012 allows an attacker to potentially read data that was not intended to be disclosed, due to the way that the Microsoft Windows EOT font engine parses specially crafted embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability."" This CVE ID is unique from CVE-2017-11835."  
  
[CVE-2017-11833] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to determine the origin of all webpages in the affected browser, due to how Microsoft Edge handles cross-origin requests, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11844."  
  
[CVE-2017-11834] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11791."  
  
[CVE-2017-11835] "Microsoft graphics in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an attacker to potentially read data that was not intended to be disclosed due to the way that the Microsoft Windows Embedded OpenType (EOT) font engine parses specially crafted embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11832."  
  
[CVE-2017-11836] "ChakraCore, and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11837] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11838] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11839] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11840] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11841] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11843] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11844] "Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11833."  
  
[CVE-2017-11845] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-11846] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11848] "Internet Explorer in Microsoft Microsoft Windows 7 SP1, Windows Server 2008 SP2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to detect the navigation of the user leaving a maliciously crafted page, due to how page content is handled by Internet Explorer, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2017-11850] "Microsoft Graphics Component in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to log on to an affected system and run a specially crafted application due to improper handling of objects in memory, aka ""Microsoft Graphics Component Information Disclosure Vulnerability""."  
  
[CVE-2017-11852] "Microsoft GDI Component in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an attacker to log on to an affected system and run a specially crafted application to compromise the user's system, due improperly disclosing kernel memory addresses, aka ""Windows GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-11855] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11856."  
  
[CVE-2017-11856] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11855."  
  
[CVE-2017-11858] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11861] "Microsoft Edge in Windows 10 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11862] "ChakraCore and Microsoft Edge in Windows 10 1709 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11863] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to trick a user into loading a page containing malicious content, due to how the Edge Content Security Policy (CSP) validates documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11872 and CVE-2017-11874."  
  
[CVE-2017-11866] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11869] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11870] "ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11871] "ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11873."  
  
[CVE-2017-11872] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to force the browser to send data that would otherwise be restricted to a destination website of the attacker's choice, due to how Microsoft Edge handles redirect requests, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11874."  
  
[CVE-2017-11873] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11871."  
  
[CVE-2017-11874] "Microsoft Edge in Microsoft Windows 10 1703, 1709, Windows Server, version 1709, and ChakraCore allows an attacker to bypass Control Flow Guard (CFG) to run arbitrary code on a target system, due to how Microsoft Edge handles accessing memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11872."  
  
[CVE-2017-11886] "Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11887] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handle objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11906 and CVE-2017-11919."  
  
[CVE-2017-11888] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-11889] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11890] "Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11893] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11894] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and and Internet Explorer adn Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11895] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11899] "Device Guard in Windows 10 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows a security feature bypass vulnerability due to the way untrusted files are handled, aka ""Microsoft Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-11901] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11903] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11905] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11906] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11919."  
  
[CVE-2017-11907] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11912] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11913] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11914] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11918] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, and CVE-2017-11930."  
  
[CVE-2017-11919] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016, and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11906."  
  
[CVE-2017-11927] "Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allow an information vulnerability due to the way the Windows its:// protocol handler determines the zone of a request, aka ""Microsoft Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-11930] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, and CVE-2017-11916."  
  
[CVE-2017-11937] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, 1709 and Windows Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to remote code execution. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-11940] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, 1709 and Windows Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to remote code execution. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"". This is different than CVE-2017-11937."  
  
[CVE-2017-12266] A vulnerability in the routine that loads DLL files in Cisco Meeting App for Windows could allow an authenticated, local attacker to run an executable file with privileges equivalent to those of Cisco Meeting App. The vulnerability is due to incomplete input validation of the path name for DLL files before they are loaded. An attacker could exploit this vulnerability by installing a crafted DLL file in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to those of Cisco Meeting App. The attacker would need valid user credentials to exploit this vulnerability. Cisco Bug IDs: CSCvd77907.  
  
[CVE-2017-12312] An untrusted search path (aka DLL Preloading) vulnerability in the Cisco Immunet antimalware installer could allow an authenticated, local attacker to execute arbitrary code via DLL hijacking if a local user with administrative privileges executes the installer in the current working directory where a crafted DLL has been placed by an attacker. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. An attacker would need valid user credentials to exploit this vulnerability. Cisco Bug IDs: CSCvf23928.  
  
[CVE-2017-12313] An untrusted search path (aka DLL Preload) vulnerability in the Cisco Network Academy Packet Tracer software could allow an authenticated, local attacker to execute arbitrary code via DLL hijacking if a local user with administrative privileges executes the installer in the current working directory where a crafted DLL has been placed by an attacker. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. An attacker would need valid user credentials to exploit this vulnerability.  
  
[CVE-2017-16744] A path traversal vulnerability in Tridium Niagara AX Versions 3.8 and prior and Niagara 4 systems Versions 4.4 and prior installed on Microsoft Windows Systems can be exploited by leveraging valid platform (administrator) credentials.  
  
[CVE-2017-3222] Hard-coded credentials in AmosConnect 8 allow remote attackers to gain full administrative privileges, including the ability to execute commands on the Microsoft Windows host platform with SYSTEM privileges by abusing AmosConnect Task Manager.  
  
[CVE-2017-3823] An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.  
  
[CVE-2017-4028] Maliciously misconfigured registry vulnerability in all Microsoft Windows products in McAfee consumer and corporate products allows an administrator to inject arbitrary code into a debugged McAfee process via manipulation of registry parameters.  
  
[CVE-2017-6638] A vulnerability in how DLL files are loaded with Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and run an executable file with privileges equivalent to the Microsoft Windows SYSTEM account. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. The attacker would need valid user credentials to exploit this vulnerability. This vulnerability affects all Cisco AnyConnect Secure Mobility Client for Windows software versions prior to 4.4.02034. Cisco Bug IDs: CSCvc97928.  
  
[CVE-2017-6639] A vulnerability in the role-based access control (RBAC) functionality of Cisco Prime Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to access sensitive information or execute arbitrary code with root privileges on an affected system. The vulnerability is due to the lack of authentication and authorization mechanisms for a debugging tool that was inadvertently enabled in the affected software. An attacker could exploit this vulnerability by remotely connecting to the debugging tool via TCP. A successful exploit could allow the attacker to access sensitive information about the affected software or execute arbitrary code with root privileges on the affected system. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM) Software Releases 10.1(1) and 10.1(2) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd09961.  
  
[CVE-2017-6640] A vulnerability in Cisco Prime Data Center Network Manager (DCNM) Software could allow an unauthenticated, remote attacker to log in to the administrative console of a DCNM server by using an account that has a default, static password. The account could be granted root- or system-level privileges. The vulnerability exists because the affected software has a default user account that has a default, static password. The user account is created automatically when the software is installed. An attacker could exploit this vulnerability by connecting remotely to an affected system and logging in to the affected software by using the credentials for this default user account. A successful exploit could allow the attacker to use this default user account to log in to the affected software and gain access to the administrative console of a DCNM server. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM) Software releases prior to Release 10.2(1) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd95346.  
  
[CVE-2017-6753] A vulnerability in Cisco WebEx browser extensions for Google Chrome and Mozilla Firefox could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server, Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center), and Cisco WebEx Meetings when they are running on Microsoft Windows. The vulnerability is due to a design defect in the extension. An attacker who can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser. The following versions of the Cisco WebEx browser extensions are affected: Versions prior to 1.0.12 of the Cisco WebEx extension on Google Chrome, Versions prior to 1.0.12 of the Cisco WebEx extension on Mozilla Firefox. Cisco Bug IDs: CSCvf15012 CSCvf15020 CSCvf15030 CSCvf15033 CSCvf15036 CSCvf15037.  
  
[CVE-2017-7269] "Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with ""If: <http://"" in a PROPFIND request, as exploited in the wild in July or August 2016."  
  
[CVE-2017-8461] "Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server which has Routing and Remote Access enabled via a specially crafted application, aka ""Windows RPC Remote Code Execution Vulnerability."""  
  
[CVE-2017-8462] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8464] "Windows Shell in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows local users or remote attackers to execute arbitrary code via a crafted .LNK file, which is not properly handled during icon display in Windows Explorer or any other application that parses the icon of the shortcut. aka ""LNK Remote Code Execution Vulnerability."""  
  
[CVE-2017-8465] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to run processes in an elevated context when the Windows kernel improperly handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability."" This CVE ID is unique from CVE-2017-8468."  
  
[CVE-2017-8467] "Graphics in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8468] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to run processes in an elevated context when the Windows kernel improperly handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability."" This CVE ID is unique from CVE-2017-8465."  
  
[CVE-2017-8469] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8470] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8471] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8472] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8473] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8474] "The kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8475] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8476] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8477] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, and CVE-2017-8484."  
  
[CVE-2017-8478] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8479] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8480] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8481] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8482] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8483] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8484] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, and CVE-2017-8477."  
  
[CVE-2017-8485] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8486] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an information disclosure due to the way it handles objects in memory, aka ""Win32k Information Disclosure Vulnerability""."  
  
[CVE-2017-8488] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8489] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8490] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8491] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8492] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8493] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to set variables that are either read-only or require authentication when Windows fails to enforce case sensitivity for certain variable checks, aka ""Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8494] "Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a locally-authenticated attacker to run a specially crafted application on a targeted system when Windows Secure Kernel Mode fails to properly handle objects in memory, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8495] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to bypass Extended Protection for Authentication when Kerberos fails to prevent tampering with the SNAME field during ticket exchange, aka ""Kerberos SNAME Security Feature Bypass Vulnerability"" or Orpheus' Lyre."  
  
[CVE-2017-8496] "Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8497."  
  
[CVE-2017-8497] "Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8496."  
  
[CVE-2017-8498] "Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read data not intended to be disclosed when Edge allows JavaScript XML DOM objects to detect installed browser extensions, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8504."  
  
[CVE-2017-8499] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8520, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8503] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to escape from the AppContainer sandbox, aka ""Microsoft Edge Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8642."  
  
[CVE-2017-8504] "Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read the URL of a cross-origin request when the Microsoft Edge Fetch API incorrectly handles a filtered response type, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8498."  
  
[CVE-2017-8515] "Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an unauthenticated attacker to send a specially crafted kernel mode request to cause a denial of service on the target system, aka ""Windows VAD Cloning Denial of Service Vulnerability""."  
  
[CVE-2017-8517] "Microsoft browsers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8522 and CVE-2017-8524."  
  
[CVE-2017-8519] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8547."  
  
[CVE-2017-8520] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8521] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8522] "Microsoft browsers in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8517 and CVE-2017-8524."  
  
[CVE-2017-8523] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge fails to correctly apply Same Origin Policy for HTML elements present in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8530 and CVE-2017-8555."  
  
[CVE-2017-8524] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8517 and CVE-2017-8522."  
  
[CVE-2017-8528] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows a remote code execution vulnerability due to the way it handles objects in memory, aka ""Windows Uniscribe Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0283."  
  
[CVE-2017-8529] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to detect specific files on the user's computer when affected Microsoft scripting engines do not properly handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2017-8530] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge does not properly enforce same-origin policies, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8555."  
  
[CVE-2017-8531] "Graphics in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 Service Pack 3, and Microsoft Office 2010 Service Pack 2 allows improper disclosure of memory contents, aka ""Graphics Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0286, CVE-2017-0287, CVE-2017-0288, CVE-2017-0289, CVE-2017-8532, and CVE-2017-8533."  
  
[CVE-2017-8534] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0284, and CVE-2017-0285."  
  
[CVE-2017-8535] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8536, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8536] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8537] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8538] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8540 and CVE-2017-8541."  
  
[CVE-2017-8539] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8542."  
  
[CVE-2017-8540] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8538 and CVE-2017-8541."  
  
[CVE-2017-8541] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8538 and CVE-2017-8540."  
  
[CVE-2017-8542] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8539."  
  
[CVE-2017-8543] "Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to take control of the affected system when Windows Search fails to handle objects in memory, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-8544] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to obtain information to further compromise the user's system when Windows Search fails to handle objects in memory, aka ""Windows Search Information Disclosure Vulnerability""."  
  
[CVE-2017-8547] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8519."  
  
[CVE-2017-8548] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8549."  
  
[CVE-2017-8549] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8548."  
  
[CVE-2017-8552] "A kernel-mode driver in Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, and Windows 8 allows an elevation of privilege when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2017-0263."  
  
[CVE-2017-8553] "An information disclosure vulnerability exists in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows Server 2016 when the Windows kernel improperly handles objects in memory, aka ""GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-8554] The kernel in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an authenticated attacker to obtain memory contents via a specially crafted application.  
  
[CVE-2017-8555] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8530."  
  
[CVE-2017-8556] "Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8574."  
  
[CVE-2017-8558] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on 32-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703 does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-8561] "Windows kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka ""Windows Kernel Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8562] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows improperly handling calls to Advanced Local Procedure Call (ALPC), aka ""Windows ALPC Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8563] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Kerberos falling back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8564] "Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly initialize a memory address, aka ""Windows Kernel Information Disclosure Vulnerability""."  
  
[CVE-2017-8566] "Microsoft Windows 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows Input Method Editor (IME) improperly handling parameters in a method of a DCOM class, aka ""Windows IME Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8573] "Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8574 and CVE-2017-8556."  
  
[CVE-2017-8574] "Graphics in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8556."  
  
[CVE-2017-8575] "The kernel in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application, aka ""Microsoft Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2017-8576] "The graphics component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability."""  
  
[CVE-2017-8577] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8578] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8577, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8579] "The DirectX component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka ""DirectX Elevation of Privilege Vulnerability."""  
  
[CVE-2017-8580] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8577, CVE-2017-8578, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8581] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8577, and CVE-2017-8467."  
  
[CVE-2017-8582] "HTTP.sys in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when the component improperly handles objects in memory, aka ""Https.sys Information Disclosure Vulnerability""."  
  
[CVE-2017-8588] "Microsoft WordPad in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way it parses specially crafted files, aka ""WordPad Remote Code Execution Vulnerability""."  
  
[CVE-2017-8589] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way that Windows Search handles objects in memory, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-8590] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way that the Windows Common Log File System (CLFS) driver handles objects in memory, aka ""Windows CLFS Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8592] "Microsoft browsers on when Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows RT 8.1, and Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a security feature bypass vulnerability when they improperly handle redirect requests, aka ""Microsoft Browser Security Feature Bypass""."  
  
[CVE-2017-8593] "Microsoft Win32k in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8594] "Internet Explorer on Microsoft Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability""."  
  
[CVE-2017-8595] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601,CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8596] "Microsoft Edge in Microsoft Windows 10 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8610, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8597] "Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8643 and CVE-2017-8648."  
  
[CVE-2017-8598] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8599] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8601] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8598 and CVE-2017-8609."  
  
[CVE-2017-8602] "Microsoft browsers on Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a spoofing vulnerability in the way they parse HTTP content, aka ""Microsoft Browser Spoofing Vulnerability."""  
  
[CVE-2017-8603] "Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8598, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8604] "Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8610, CVE-2017-8603, CVE-2017-8598, CVE-2017-8601, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8605] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8598, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8606] "Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609"  
  
[CVE-2017-8607] "Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8608, and CVE-2017-8609"  
  
[CVE-2017-8608] "Microsoft browsers in Microsoft Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8607, and CVE-2017-8609"  
  
[CVE-2017-8609] "Microsoft Internet Explorer in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Internet Explorer, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8610] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8595, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8611] "Microsoft Edge on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote attackers to spoof web content via a crafted web site, aka ""Microsoft Edge Spoofing Vulnerability."""  
  
[CVE-2017-8617] "Microsoft Edge in Windows 10 1703 Microsoft Edge allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Microsoft Edge Remote Code Execution Vulnerability."""  
  
[CVE-2017-8618] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 Internet Explorer in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability."" This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8619, CVE-2017-9598 and CVE-2017-8609."  
  
[CVE-2017-8619] "Microsoft Edge on Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability."" This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8618, CVE-2017-9598 and CVE-2017-8609."  
  
[CVE-2017-8628] "Microsoft Bluetooth Driver in Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 allows a spoofing vulnerability due to Microsoft's implementation of the Bluetooth stack, aka ""Microsoft Bluetooth Driver Spoofing Vulnerability""."  
  
[CVE-2017-8634] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8635] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that JavaScript engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8636] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8637] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to bypass Arbitrary Code Guard (ACG) due to how Microsoft Edge accesses memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka ""Scripting Engine Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8638] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8639] "Microsoft Edge in Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8640] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8641] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8642] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to elevate privileges due to the way that Microsoft Edge validates JavaScript under specific conditions, aka ""Microsoft Edge Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8503."  
  
[CVE-2017-8643] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to leave a malicious website open during user clipboard activities, due to the way that Microsoft Edge handles clipboard events, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8648."  
  
[CVE-2017-8644] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8652 and CVE-2017-8662."  
  
[CVE-2017-8645] "Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8646] "Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8647] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8648] "Microsoft Edge in Microsoft Windows Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8643."  
  
[CVE-2017-8649] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8650] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to exploit a security feature bypass due to Microsoft Edge not properly enforcing same-origin policies, aka ""Microsoft Edge Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8651] "Internet Explorer in Microsoft Windows Server 2008 SP2 and Windows Server 2012 allows an attacker to execute arbitrary code in the context of the current user due to Internet Explorer improperly accessing objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability""."  
  
[CVE-2017-8652] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8662."  
  
[CVE-2017-8653] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to Microsoft browsers improperly accessing objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8669."  
  
[CVE-2017-8655] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8656] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8657] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8659] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system due to the Chakra scripting engine not properly handling objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability""."  
  
[CVE-2017-8660] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8661] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way affected Microsoft scripting engines render when handling objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-8662] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to disclose information due to how strings are validated in specific scenarios, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8652."  
  
[CVE-2017-8666] "Microsoft Win32k in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly handle objects in memory, aka ""Win32k Information Disclosure Vulnerability""."  
  
[CVE-2017-8668] "The Volume Manager Extension Driver in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2 allows an attacker to run a specially crafted application and obtain kernel information, aka ""Volume Manager Extension Driver Information Disclosure Vulnerability""."  
  
[CVE-2017-8669] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to Microsoft browsers improperly handling objects in memory while rendering content, aka ""Microsoft Browser Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8653."  
  
[CVE-2017-8670] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8671] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8672] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8674."  
  
[CVE-2017-8673] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 10 1703 allows an attacker to connect to a target system using RDP and send specially crafted requests, aka ""Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability."""  
  
[CVE-2017-8674] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8672."  
  
[CVE-2017-8675] "The Windows Kernel-Mode Drivers component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when the Win32k component fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"".. This CVE ID is unique from CVE-2017-8720."  
  
[CVE-2017-8676] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8677] "The Windows GDI+ component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly discloses kernel memory addresses, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8678] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8677, CVE-2017-8680, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8679] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8709, and CVE-2017-8719."  
  
[CVE-2017-8680] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8677, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8681] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8677, and CVE-2017-8687."  
  
[CVE-2017-8682] "Windows graphics on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, Windows Server 2016, Microsoft Office Word Viewer, Microsoft Office 2007 Service Pack 3 , and Microsoft Office 2010 Service Pack 2 allows an attacker to execute remote code by the way it handles embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8683."  
  
[CVE-2017-8683] "Windows graphics on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an attacker to execute remote code by the way it handles embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8682."  
  
[CVE-2017-8684] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1, allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8685 and CVE-2017-8688."  
  
[CVE-2017-8685] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8684 and CVE-2017-8688."  
  
[CVE-2017-8687] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8677, and CVE-2017-8681."  
  
[CVE-2017-8688] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8684 and CVE-2017-8685."  
  
[CVE-2017-8689] "The Microsoft Windows Kernel Mode Driver on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8694."  
  
[CVE-2017-8692] "The Windows Uniscribe component on Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote code execution vulnerability when it fails to properly handle objects in memory, aka ""Uniscribe Remote Code Execution Vulnerability""."  
  
[CVE-2017-8693] "The Microsoft Graphics Component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability in the way it handles objects in memory, aka ""Microsoft Graphics Information Disclosure Vulnerability""."  
  
[CVE-2017-8694] "The Microsoft Windows Kernel Mode Driver on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8689."  
  
[CVE-2017-8695] "Windows Uniscribe in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8696] "Windows Uniscribe in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8699] "Windows Shell in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to run arbitrary code in the context of the current user, due to the way that Windows Shell validates file copy destinations, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2017-8702] "Windows Error Reporting (WER) in Microsoft Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows an attacker to gain greater access to sensitive information and system functionality, due to the way that WER handles and executes files, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8703] "The Microsoft Windows Subsystem for Linux on Microsoft Windows 10 1703 allows a denial of service vulnerability when it improperly handles objects in memory, aka ""Windows Subsystem for Linux Denial of Service Vulnerability""."  
  
[CVE-2017-8704] "The Windows Hyper-V component on Microsoft Windows 10 1607 and Windows Server 2016 allows a denial of service vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability""."  
  
[CVE-2017-8706] "The Windows Hyper-V component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8707] "The Windows Hyper-V component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8706, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8708] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8679, CVE-2017-8709, and CVE-2017-8719."  
  
[CVE-2017-8709] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8679, and CVE-2017-8719."  
  
[CVE-2017-8710] "The Microsoft Common Console Document (.msc) in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1 allows an attacker to read arbitrary files via an XML external entity (XXE) declaration, due to the way that the Microsoft Common Console Document (.msc) parses XML input containing a reference to an external entity, aka ""Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-8711] "The Windows Hyper-V component on Microsoft Windows 10 1607 and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8706, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8712] "The Windows Hyper-V component on Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8706, and CVE-2017-8713."  
  
[CVE-2017-8713] "The Windows Hyper-V component on Microsoft Windows Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8706."  
  
[CVE-2017-8714] "The Windows Hyper-V component on Microsoft Windows 8.1, Windows Server 2012 Gold and R2,, Windows 10 1607, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Remote Desktop Virtual Host Remote Code Execution Vulnerability""."  
  
[CVE-2017-8715] "The Microsoft Device Guard on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass by the way it handles Windows PowerShell sessions, aka ""Windows Security Feature Bypass""."  
  
[CVE-2017-8716] "Windows Control Flow Guard in Microsoft Windows 10 Version 1703 allows an attacker to run a specially crafted application to bypass Control Flow Guard, due to the way that Control Flow Guard handles objects in memory, aka ""Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8717] "The Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to take control of an affected system, due to how it handles objects in memory, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8718."  
  
[CVE-2017-8718] "The Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to take control of an affected system, due to how it handles objects in memory, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8717."  
  
[CVE-2017-8719] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8709, and CVE-2017-8679."  
  
[CVE-2017-8720] "The Microsoft Windows graphics component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when the Win32k component fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8675."  
  
[CVE-2017-8723] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8754."  
  
[CVE-2017-8724] "Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka ""Microsoft Edge Spoofing Vulnerability"". This CVE ID is unique from CVE-2017-8735."  
  
[CVE-2017-8726] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how affected Microsoft scripting engines handle objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11794 and CVE-2017-11803."  
  
[CVE-2017-8727] "Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Windows Text Services Framework handles objects in memory, aka ""Windows Shell Memory Corruption Vulnerability""."  
  
[CVE-2017-8728] "Microsoft Windows PDF Library in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Windows PDF Library handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8737."  
  
[CVE-2017-8729] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8731] "Microsoft Edge in Microsoft Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8734, CVE-2017-8751, and CVE-2017-11766."  
  
[CVE-2017-8733] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into believing that the user was visiting a legitimate website, due to the way that Internet Explorer handles specific HTML content, aka ""Internet Explorer Spoofing Vulnerability""."  
  
[CVE-2017-8734] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8751, and CVE-2017-11766."  
  
[CVE-2017-8735] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka ""Microsoft Edge Spoofing Vulnerability"". This CVE ID is unique from CVE-2017-8724."  
  
[CVE-2017-8736] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to obtain specific information used in the parent domain, due to Microsoft browser parent domain verification in certain functionality, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2017-8737] "Microsoft Windows PDF Library in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Windows PDF Library handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8728."  
  
[CVE-2017-8738] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8739] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability""."  
  
[CVE-2017-8740] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8741] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8747] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Internet Explorer accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8749."  
  
[CVE-2017-8748] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8749] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Internet Explorer accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8747."  
  
[CVE-2017-8750] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browsers access objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability""."  
  
[CVE-2017-8751] "Microsoft Edge in Microsoft Windows 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-11766."  
  
[CVE-2017-8752] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8753] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8754] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8723."  
  
[CVE-2017-8755] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the scripting engine handles objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8756] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-11764."  
  
[CVE-2017-8757] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way Microsoft Edge handles objects in memory, aka ""Microsoft Edge Remote Code Execution Vulnerability""."  
  
[CVE-2017-9511] The MultiPathResource class in Atlassian Fisheye and Crucible, before version 4.4.1 allows anonymous remote attackers to read arbitrary files via a path traversal vulnerability when Fisheye or Crucible is running on the Microsoft Windows operating system.  
  
[CVE-2018-0598] Untrusted search path vulnerability in Self-extracting archive files created by IExpress bundled with Microsoft Windows allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.  
  
[CVE-2018-0741] "The Color Management Module (Icm32.dll) in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an information disclosure vulnerability due to the way objects are handled in memory, aka ""Microsoft Color Management Information Disclosure Vulnerability""."  
  
[CVE-2018-0749] "The Microsoft Server Message Block (SMB) Server in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way SMB Server handles specially crafted files, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0755] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0760, CVE-2018-0761, and CVE-2018-0855."  
  
[CVE-2018-0758] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0760] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1, Windows Server 2008 R2, and Windows Server 2012 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0761, and CVE-2018-0855."  
  
[CVE-2018-0761] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0760, and CVE-2018-0855."  
  
[CVE-2018-0762] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0763] "Microsoft Edge in Microsoft Windows 10 1703 and 1709 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0839."  
  
[CVE-2018-0766] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the Microsoft Edge PDF Reader handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability""."  
  
[CVE-2018-0767] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0780 and CVE-2018-0800."  
  
[CVE-2018-0768] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0769] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0770] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0771] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows a security feature bypass, due to how Edge handles different-origin requests, aka ""Microsoft Edge Security Feature Bypass""."  
  
[CVE-2018-0772] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0773] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0774] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0775] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0776] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0777] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0778] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0781."  
  
[CVE-2018-0780] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0800."  
  
[CVE-2018-0781] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0778."  
  
[CVE-2018-0800] "Microsoft Edge in Microsoft Windows 10 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0780."  
  
[CVE-2018-0803] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to access information from one domain and inject it into another domain, due to how Microsoft Edge enforces cross-domain policies, aka ""Microsoft Edge Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0811] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0813] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0814] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0815] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Windows 7 SP1 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0816, and CVE-2018-0817."  
  
[CVE-2018-0816] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0815 and CVE-2018-0817."  
  
[CVE-2018-0817] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0815 and CVE-2018-0816."  
  
[CVE-2018-0824] "A remote code execution vulnerability exists in ""Microsoft COM for Windows"" when it fails to properly handle serialized objects, aka ""Microsoft COM for Windows Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-0833] "The Microsoft Server Message Block 2.0 and 3.0 (SMBv2/SMBv3) client in Windows 8.1 and RT 8.1 and Windows Server 2012 R2 allows a denial of service vulnerability due to how specially crafted requests are handled, aka ""SMBv2/SMBv3 Null Dereference Denial of Service Vulnerability""."  
  
[CVE-2018-0834] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0835] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0836] "Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0837] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0838] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0839] "Microsoft Edge in Microsoft Windows 10 1703 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0763."  
  
[CVE-2018-0840] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0847] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2018-0855] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0760, and CVE-2018-0761."  
  
[CVE-2018-0856] "Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0857] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0859] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0860] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0861] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, and CVE-2018-0866."  
  
[CVE-2018-0866] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, and CVE-2018-0861."  
  
[CVE-2018-0868] "Windows Installer in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to how input is sanitized, aka ""Windows Installer Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0872] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0873] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0874] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0876] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0889, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0878] "Windows Remote Assistance in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to how XML External Entities (XXE) are processed, aka ""Windows Remote Assistance Information Disclosure Vulnerability""."  
  
[CVE-2018-0879] "Microsoft Edge in Windows 10 1709 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability""."  
  
[CVE-2018-0881] "The Microsoft Video Control in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege due to how objects are handled in memory, aka ""Microsoft Video Control Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0883] "Windows Shell in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how file copy destinations are validated, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2018-0885] "The Microsoft Hyper-V Network Switch in 64-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows a denial of service vulnerability due to how input from a privileged user on a guest operating system is validated, aka ""Hyper-V Denial of Service Vulnerability""."  
  
[CVE-2018-0886] "The Credential Security Support Provider protocol (CredSSP) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709 Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how CredSSP validates request during the authentication process, aka ""CredSSP Remote Code Execution Vulnerability""."  
  
[CVE-2018-0888] "The Microsoft Hyper-V Network Switch in 64-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to how guest operating system input is validated, aka ""Hyper-V Information Disclosure Vulnerability""."  
  
[CVE-2018-0889] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0891] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0939."  
  
[CVE-2018-0893] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0889, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0894] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0895] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0896] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0897] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0898] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0899] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0900] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0901] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0926."  
  
[CVE-2018-0904] "The Windows kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure vulnerability due to how memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability""."  
  
[CVE-2018-0926] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901."  
  
[CVE-2018-0927] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2018-0929] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2018-0930] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1709 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0931] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0932] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2018-0933] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0934] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0935] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0889, CVE-2018-0893, and CVE-2018-0925."  
  
[CVE-2018-0936] "ChakraCore and Microsoft Windows 10 1709 allow remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, and CVE-2018-0937."  
  
[CVE-2018-0937] "ChakraCore and Microsoft Windows 10 1703 and 1709 allow remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, and CVE-2018-0936."  
  
[CVE-2018-0939] "ChakraCore and Microsoft Edge in Windows 10 1703 and 1709 allow information disclosure, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0891."  
  
[CVE-2018-0942] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow elevation of privilege, due to how Internet Explorer handles zone and integrity settings, aka ""Internet Explorer Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0952] "An Elevation of Privilege vulnerability exists when Diagnostics Hub Standard Collector allows file creation in arbitrary locations, aka ""Diagnostic Hub Standard Collector Elevation Of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Microsoft Visual Studio, Windows 10 Servers."  
  
[CVE-2018-0986] "A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption, aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability."" This affects Windows Defender, Windows Intune Endpoint Protection, Microsoft Security Essentials, Microsoft System Center Endpoint Protection, Microsoft Exchange Server, Microsoft System Center, Microsoft Forefront Endpoint Protection."  
  
[CVE-2018-1003] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10."  
  
[CVE-2018-1009] "An elevation of privilege vulnerability exists when Windows improperly handles objects in memory and incorrectly maps kernel memory, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-1010] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1012, CVE-2018-1013, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1012] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1013, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1013] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1015] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1016."  
  
[CVE-2018-1016] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1015."  
  
[CVE-2018-13399] The Microsoft Windows Installer for Atlassian Fisheye and Crucible before version 4.6.1 allows local attackers to escalate privileges because of weak permissions on the installation directory.  
  
[CVE-2018-15408] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15409] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15410] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15411] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15412] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15413] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15414] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15415] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15416] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15417] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15418] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15419] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15420] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15421] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15422] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15431] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15437] A vulnerability in the system scanning component of Cisco Immunet and Cisco Advanced Malware Protection (AMP) for Endpoints running on Microsoft Windows could allow a local attacker to disable the scanning functionality of the product. This could allow executable files to be launched on the system without being analyzed for threats. The vulnerability is due to improper process resource handling. An attacker could exploit this vulnerability by gaining local access to a system running Microsoft Windows and protected by Cisco Immunet or Cisco AMP for Endpoints and executing a malicious file. A successful exploit could allow the attacker to prevent the scanning services from functioning properly and ultimately prevent the system from being protected from further intrusion.  
  
[CVE-2018-15490] An issue was discovered in ExpressVPN on Windows. The Xvpnd.exe process (which runs as a service with SYSTEM privileges) listens on TCP port 2015, which is used as an RPC interface for communication with the client side of the ExpressVPN application. A JSON-RPC protocol over HTTP is used for communication. The JSON-RPC XVPN.GetPreference and XVPN.SetPreference methods are vulnerable to path traversal, and allow reading and writing files on the file system on behalf of the service.  
  
[CVE-2018-16794] Microsoft ADFS 4.0 Windows Server 2016 and previous (Active Directory Federation Services) has an SSRF vulnerability via the txtBoxEmail parameter in /adfs/ls.  
  
[CVE-2018-3700] Code injection vulnerability in the installer for Intel(R) USB 3.0 eXtensible Host Controller Driver for Microsoft Windows 7 before version 5.0.4.43v2 may allow a user to potentially enable escalation of privilege via local access.  
  
[CVE-2018-4858] A vulnerability has been identified in IEC 61850 system configurator (All versions < V5.80), DIGSI 5 (affected as IEC 61850 system configurator is incorporated) (All versions < V7.80), DIGSI 4 (All versions < V4.93), SICAM PAS/PQS (All versions < V8.11), SICAM PQ Analyzer (All versions < V3.11), SICAM SCC (All versions < V9.02 HF3). A service of the affected products listening on all of the host's network interfaces on either port 4884/TCP, 5885/TCP, or port 5886/TCP could allow an attacker to either exfiltrate limited data from the system or to execute code with Microsoft Windows user permissions. Successful exploitation requires an attacker to be able to send a specially crafted network request to the vulnerable service and a user interacting with the service's client application on the host. In order to execute arbitrary code with Microsoft Windows user permissions, an attacker must be able to plant the code in advance on the host by other means. The vulnerability has limited impact to confidentiality and integrity of the affected system. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.  
  
[CVE-2018-5440] A Stack-based Buffer Overflow issue was discovered in 3S-Smart CODESYS Web Server. Specifically: all Microsoft Windows (also WinCE) based CODESYS web servers running stand-alone Version 2.3, or as part of the CODESYS runtime system running prior to Version V1.1.9.19. A crafted request may cause a buffer overflow and could therefore execute arbitrary code on the web server or lead to a denial-of-service condition due to a crash in the web server.  
  
[CVE-2018-6661] DLL Side-Loading vulnerability in Microsoft Windows Client in McAfee True Key before 4.20.110 allows local users to gain privilege elevation via not verifying a particular DLL file signature.  
  
[CVE-2018-6664] Application Protections Bypass vulnerability in Microsoft Windows in McAfee Data Loss Prevention (DLP) Endpoint before 10.0.500 and DLP Endpoint before 11.0.400 allows authenticated users to bypass the product block action via a command-line utility.  
  
[CVE-2018-6674] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 13 allows local users to spawn unrelated processes with elevated privileges via the system administrator granting McTray.exe elevated privileges (by default it runs with the current user's privileges).  
  
[CVE-2018-6687] Loop with Unreachable Exit Condition ('Infinite Loop') in McAfee GetSusp (GetSusp) 3.0.0.461 and earlier allows attackers to DoS a manual GetSusp scan via while scanning a specifically crafted file . GetSusp is a free standalone McAfee tool that runs on several versions of Microsoft Windows.  
  
[CVE-2018-6690] Accessing, modifying, or executing executable files vulnerability in Microsoft Windows client in McAfee Application and Change Control (MACC) 8.0.0 Hotfix 4 and earlier allows authenticated users to execute arbitrary code via file transfer from external system.  
  
[CVE-2018-6700] DLL Search Order Hijacking vulnerability in Microsoft Windows Client in McAfee True Key (TK) before 5.1.165 allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6755] Weak Directory Permission Vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6756] Authentication Abuse vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute unauthorized commands via specially crafted malware.  
  
[CVE-2018-6757] Privilege Escalation vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6765] Swisscom MySwisscomAssistant 2.17.1.1065 contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system. This vulnerability exists due to the way .dll files are loaded. It allows an attacker to load a .dll of the attacker's choosing that could execute arbitrary code without the user's knowledge. The specific flaw exists within the handling of several DLLs (dwmapi.dll, IPHLPAPI.DLL, WindowsCodecs.dll, RpcRtRemote.dll, CRYPTSP.dll, rasadhlp.dll, DNSAPI.dll, ntmarta.dll, netbios.dll, olepro32.dll, security.dll, winhttp.dll, WINSTA.dll) loaded by the MySwisscomAssistant\_Setup.exe process.  
  
[CVE-2018-7249] An issue was discovered in secdrv.sys as shipped in Microsoft Windows Vista, Windows 7, Windows 8, and Windows 8.1 before KB3086255, and as shipped in Macrovision SafeDisc. Two carefully timed calls to IOCTL 0xCA002813 can cause a race condition that leads to a use-after-free. When exploited, an unprivileged attacker can run arbitrary code in the kernel.  
  
[CVE-2018-7250] An issue was discovered in secdrv.sys as shipped in Microsoft Windows Vista, Windows 7, Windows 8, and Windows 8.1 before KB3086255, and as shipped in Macrovision SafeDisc. An uninitialized kernel pool allocation in IOCTL 0xCA002813 allows a local unprivileged attacker to leak 16 bits of uninitialized kernel PagedPool data.  
  
[CVE-2018-8116] "A denial of service vulnerability exists in the way that Windows handles objects in memory, aka ""Microsoft Graphics Component Denial of Service Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8218] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers."  
  
[CVE-2018-8253] "An elevation of privilege vulnerability exists when Microsoft Cortana allows arbitrary website browsing on the lockscreen, aka ""Microsoft Cortana Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10."  
  
[CVE-2018-8256] "A remote code execution vulnerability exists when PowerShell improperly handles specially crafted files, aka ""Microsoft PowerShell Remote Code Execution Vulnerability."" This affects Windows RT 8.1, PowerShell Core 6.0, Microsoft.PowerShell.Archive 1.2.2.0, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, Windows Server 2019, Windows 7, Windows Server 2012 R2, PowerShell Core 6.1, Windows 10 Servers, Windows 10, Windows 8.1."  
  
[CVE-2018-8307] "A security feature bypass vulnerability exists when Microsoft WordPad improperly handles embedded OLE objects, aka ""WordPad Security Feature Bypass Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8332] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Microsoft Office, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8333] "An Elevation of Privilege vulnerability exists in Filter Manager when it improperly handles objects in memory, aka ""Microsoft Filter Manager Elevation Of Privilege Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8335] "A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8344] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8345] "A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka ""LNK Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8346."  
  
[CVE-2018-8346] "A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka ""LNK Remote Code Execution Vulnerability."" This affects Windows Server 2008, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8345."  
  
[CVE-2018-8347] "An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka ""Windows Kernel Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8349] "A remote code execution vulnerability exists in ""Microsoft COM for Windows"" when it fails to properly handle serialized objects, aka ""Microsoft COM for Windows Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8350] "A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability."" This affects Windows 10 Servers, Windows 10."  
  
[CVE-2018-8392] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8393."  
  
[CVE-2018-8393] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8392."  
  
[CVE-2018-8407] "An information disclosure vulnerability exists when ""Kernel Remote Procedure Call Provider"" driver improperly initializes objects in memory, aka ""MSRPC Information Disclosure Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8415] "A tampering vulnerability exists in PowerShell that could allow an attacker to execute unlogged code, aka ""Microsoft PowerShell Tampering Vulnerability."" This affects Windows 7, PowerShell Core 6.1, Windows Server 2012 R2, Windows RT 8.1, PowerShell Core 6.0, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8417] "A security feature bypass vulnerability exists in Microsoft JScript that could allow an attacker to bypass Device Guard, aka ""Microsoft JScript Security Feature Bypass Vulnerability."" This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers."  
  
[CVE-2018-8420] "A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka ""MS XML Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8423] "A remote code execution vulnerability exists in the Microsoft JET Database Engine, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8427] "An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Information Disclosure Vulnerability."" This affects Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Windows Server 2008, Microsoft PowerPoint Viewer, Microsoft Excel Viewer."  
  
[CVE-2018-8432] "A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Remote Code Execution Vulnerability."" This affects Windows 7, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft Excel Viewer, Microsoft PowerPoint Viewer, Windows Server 2019, Windows Server 2008 R2, Windows 10, Windows Server 2008."  
  
[CVE-2018-8433] "An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka ""Microsoft Graphics Component Information Disclosure Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8436] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8437, CVE-2018-8438."  
  
[CVE-2018-8437] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8436, CVE-2018-8438."  
  
[CVE-2018-8438] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8436, CVE-2018-8437."  
  
[CVE-2018-8444] "An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability."" This affects Windows Server 2012, Windows 10, Windows 8.1, Windows RT 8.1, Windows Server 2012 R2."  
  
[CVE-2018-8471] "An elevation of privilege vulnerability exists in the way that the Microsoft RemoteFX Virtual GPU miniport driver handles objects in memory, aka ""Microsoft RemoteFX Virtual GPU miniport driver Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Windows 8.1, Windows 7, Windows Server 2019."  
  
[CVE-2018-8494] "A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka ""MS XML Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8506] "An Information Disclosure vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka ""Microsoft Windows Codecs Library Information Disclosure Vulnerability."" This affects Windows 10 Servers, Windows 10, Windows Server 2019."  
  
[CVE-2018-8547] "A cross-site-scripting (XSS) vulnerability exists when an open source customization for Microsoft Active Directory Federation Services (AD FS) does not properly sanitize a specially crafted web request to an affected AD FS server, aka ""Active Directory Federation Services XSS Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8553] "A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10."  
  
[CVE-2018-8599] "An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka ""Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability."" This affects Microsoft Visual Studio, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8634] "A remote code execution vulnerability exists in Windows where Microsoft text-to-speech fails to properly handle objects in the memory, aka ""Microsoft Text-To-Speech Remote Code Execution Vulnerability."" This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers."  
  
[CVE-2018-8853] Philips Brilliance CT devices operate user functions from within a contained kiosk in a Microsoft Windows operating system. Windows boots by default with elevated Windows privileges, enabling a kiosk application, user, or an attacker to potentially attain unauthorized elevated privileges in Brilliance 64 version 2.6.2 and prior, Brilliance iCT versions 4.1.6 and prior, Brillance iCT SP versions 3.2.4 and prior, and Brilliance CT Big Bore 2.3.5 and prior. Also, attackers may gain access to unauthorized resources from the underlying Windows operating system.  
  
[CVE-2019-0232] When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).  
  
[CVE-2019-0543] "An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka ""Microsoft Windows Elevation of Privilege Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2019-0555] "An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka ""Microsoft XmlDocument Elevation of Privilege Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2019-0630] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.  
  
[CVE-2019-0633] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630.  
  
[CVE-2019-0690] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701.  
  
[CVE-2019-0695] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0701.  
  
[CVE-2019-0701] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0695.  
  
[CVE-2019-0710] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713.  
  
[CVE-2019-0711] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713.  
  
[CVE-2019-0712] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399.  
  
[CVE-2019-0713] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711.  
  
[CVE-2019-0714] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0715, CVE-2019-0717, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0715] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0717, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0717] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0718] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0717, CVE-2019-0723.  
  
[CVE-2019-0723] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0717, CVE-2019-0718.  
  
[CVE-2019-0734] An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936.  
  
[CVE-2019-0766] An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2019-0885] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2019-0928] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2019-0936] An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734.  
  
[CVE-2019-0966] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2019-1019] A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1040] A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.  
  
[CVE-2019-1074] An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic link attack. An attacker who successfully exploited this vulnerability could potentially access unauthorized information. The update addresses this vulnerability by not allowing symbolic links in these scenarios., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1082.  
  
[CVE-2019-1078] An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1148, CVE-2019-1153.  
  
[CVE-2019-1082] An elevation of privilege vulnerability exists in Microsoft Windows where a certain DLL, with Local Service privilege, is vulnerable to race planting a customized DLL.An attacker who successfully exploited this vulnerability could potentially elevate privilege to SYSTEM.The update addresses this vulnerability by requiring SYSTEM privileges for a certain DLL., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1074.  
  
[CVE-2019-1089] An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this vulnerability, a low level authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how rpcss.dll handles these requests., aka 'Windows RPCSS Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1144] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1145] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1148] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1078, CVE-2019-1153.  
  
[CVE-2019-1149] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1150] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1151] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1152.  
  
[CVE-2019-1152] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151.  
  
[CVE-2019-1153] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1078, CVE-2019-1148.  
  
[CVE-2019-1166] A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.  
  
[CVE-2019-1168] An elevation of privilege exists in the p2pimsvc service where an attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges.To exploit this vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability'.  
  
[CVE-2019-11684] "Improper Access Control in the RCP+ server of the Bosch Video Recording Manager (VRM) component allows arbitrary and unauthenticated access to a limited subset of certificates, stored in the underlying Microsoft Windows operating system. The fixed versions implement modified authentication checks. Prior releases of VRM software version 3.70 are considered unaffected. This vulnerability affects VRM v3.70.x, v3.71 < v3.71.0034 and v3.81 < 3.81.0050  
[CVE-2019-1172] An information disclosure vulnerability exists in Azure Active Directory (AAD) Microsoft Account (MSA) during the login request session, aka 'Windows Information Disclosure Vulnerability'.  
  
[CVE-2019-1177] An elevation of privilege vulnerability exists in the way that the rpcss.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1173, CVE-2019-1174, CVE-2019-1175, CVE-2019-1178, CVE-2019-1179, CVE-2019-1180, CVE-2019-1184, CVE-2019-1186.  
  
[CVE-2019-1188] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2019-1198] An elevation of privilege exists in SyncController.dll, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1270] An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Microsoft Windows Store Installer Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1280] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2019-1309] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1310, CVE-2019-1399.  
  
[CVE-2019-1310] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1399.  
  
[CVE-2019-1316] An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1317] A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.  
  
[CVE-2019-1318] A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.  
  
[CVE-2019-1320] An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.  
  
[CVE-2019-1321] An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL), aka 'Microsoft Windows CloudStore Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1322] An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.  
  
[CVE-2019-1323] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.  
  
[CVE-2019-1336] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.  
  
[CVE-2019-1338] A security feature bypass vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLMv2 protection if a client is also sending LMv2 responses, aka 'Windows NTLM Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1340] An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1322.  
  
[CVE-2019-1381] An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'.  
  
[CVE-2019-1384] A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1399] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310.  
  
[CVE-2019-1409] An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'.  
  
[CVE-2019-1419] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456.  
  
[CVE-2019-1430] A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'Microsoft Windows Media Foundation Remote Code Execution Vulnerability'.  
  
[CVE-2019-1456] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419.  
  
[CVE-2019-1484] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2019-15162] rpcapd/daemon.c in libpcap before 1.9.1 on non-Windows platforms provides details about why authentication failed, which might make it easier for attackers to enumerate valid usernames.  
  
[CVE-2019-15283] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15284] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15285] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15286] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15287] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1637] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1638] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1639] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1640] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1641] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1771] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1772] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1773] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-18232] SafeNet Sentinel LDK License Manager, all versions prior to 7.101(only Microsoft Windows versions are affected) is vulnerable when configured as a service. This vulnerability may allow an attacker with local access to create, write, and/or delete files in system folder using symbolic links, leading to a privilege escalation. This vulnerability could also be used by an attacker to execute a malicious DLL, which could impact the integrity and availability of the system.  
  
[CVE-2019-18631] The Windows component of Centrify Authentication and Privilege Elevation Services 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.5.0, 3.5.1 (18.8), 3.5.2 (18.11), and 3.6.0 (19.6) does not properly handle an unspecified exception during use of partially trusted assemblies to serialize input data, which allows attackers to execute arbitrary code inside the Centrify process via (1) a crafted application that makes a pipe connection to the process and sends malicious serialized data or (2) a crafted Microsoft Management Console snap-in control file.  
  
[CVE-2019-18913] "A potential security vulnerability with pre-boot DMA may allow unauthorized UEFI code execution using open-case attacks. This industry-wide issue requires physically accessing internal expansion slots with specialized hardware and software tools to modify UEFI code in memory. This affects HP Intel-based Business PCs that support Microsoft Windows 10 Kernel DMA protection. Affected versions depend on platform (prior to 01.04.02  
[CVE-2019-1924] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1925] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1926] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1927] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1928] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1929] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-19363] An issue was discovered in Ricoh (including Savin and Lanier) Windows printer drivers prior to 2020 that allows attackers local privilege escalation. Affected drivers and versions are: PCL6 Driver for Universal Print - Version 4.0 or later PS Driver for Universal Print - Version 4.0 or later PC FAX Generic Driver - All versions Generic PCL5 Driver - All versions RPCS Driver - All versions PostScript3 Driver - All versions PCL6 (PCL XL) Driver - All versions RPCS Raster Driver - All version  
  
[CVE-2019-20406] The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.  
  
[CVE-2019-2390] "An unprivileged user or program on Microsoft Windows which can create OpenSSL configuration files in a fixed location may cause utility programs shipped with MongoDB server to run attacker defined code as the user running the utility. This issue affects: MongoDB Inc. MongoDB Server 4.0 prior to 4.0.11  
[CVE-2019-3582] Privilege Escalation vulnerability in Microsoft Windows client in McAfee Endpoint Security (ENS) 10.6.1 and earlier allows local users to gain elevated privileges via a specific set of circumstances.  
  
[CVE-2019-3585] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow local users to interact with the On-Access Scan Messages - Threat Alert Window with elevated privileges via running McAfee Tray with elevated privileges.  
  
[CVE-2019-3587] DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.18 allows local users to execute arbitrary code via execution from a compromised folder.  
  
[CVE-2019-3588] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow unauthorized users to interact with the On-Access Scan Messages - Threat Alert Window when the Windows Login Screen is locked.  
  
[CVE-2019-3593] Exploitation of Privilege/Trust vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.R18 allows local users to bypass product self-protection, tamper with policies and product files, and uninstall McAfee software without permission via specially crafted malware.  
  
[CVE-2019-3610] Data Leakage Attacks vulnerability in Microsoft Windows client in McAfee True Key (TK) 3.1.9211.0 and earlier allows local users to expose confidential data via specially crafted malware.  
  
[CVE-2019-3646] DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Free Antivirus Trial 16.0.R18 and earlier allows local users to execute arbitrary code via execution from a compromised folder placed by an attacker with administrator rights.  
  
[CVE-2019-3648] A Privilege Escalation vulnerability in the Microsoft Windows client in McAfee Total Protection 16.0.R22 and earlier allows administrators to execute arbitrary code via carefully placing malicious files in specific locations protected by administrator permission.  
  
[CVE-2019-3654] Authentication Bypass vulnerability in the Microsoft Windows client in McAfee Client Proxy (MCP) prior to 3.0.0 allows local user to bypass scanning of web traffic and gain access to blocked sites for a short period of time via generating an authorization key on the client which should only be generated by the network administrator.  
  
[CVE-2019-3667] DLL Search Order Hijacking vulnerability in the Microsoft Windows client in McAfee Tech Check 3.0.0.17 and earlier allows local users to execute arbitrary code via the local folder placed there by an attacker.  
  
[CVE-2019-3880] A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.  
  
[CVE-2019-4732] IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.  
  
[CVE-2019-6265] The Scripting and AutoUpdate functionality in Cordaware bestinformed Microsoft Windows client versions before 6.2.1.0 are affected by insecure implementations which allow remote attackers to execute arbitrary commands and escalate privileges.  
  
[CVE-2019-6266] Cordaware bestinformed Microsoft Windows client before 6.2.1.0 is affected by insecure SSL certificate verification and insecure access patterns. These issues allow remote attackers to downgrade encrypted connections to cleartext.  
  
[CVE-2019-9510] A vulnerability in Microsoft Windows 10 1803 and Windows Server 2019 and later systems can allow authenticated RDP-connected clients to gain access to user sessions without needing to interact with the Windows lock screen. Should a network anomaly trigger a temporary RDP disconnect, Automatic Reconnection of the RDP session will be restored to an unlocked state, regardless of how the remote system was left. By interrupting network connectivity of a system, an attacker with access to a system being used as a Windows RDP client can gain access to a connected remote system, regardless of whether or not the remote system was locked. This issue affects Microsoft Windows 10, version 1803 and later, and Microsoft Windows Server 2019, version 2019 and later.  
  
[CVE-2020-0616] A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.  
  
[CVE-2020-0622] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-0635] An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0644.  
  
[CVE-2020-0641] An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-0644] An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0635.  
  
[CVE-2020-0661] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751.  
  
[CVE-2020-0684] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-0687] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.  
  
[CVE-2020-0729] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-0751] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0661.  
  
[CVE-2020-0796] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.  
  
[CVE-2020-0799] An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka 'Windows Kernel Elevation of Privilege Vulnerability'.  
  
[CVE-2020-0890] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0904.  
  
[CVE-2020-0904] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0890.  
  
[CVE-2020-0921] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1083.  
  
[CVE-2020-0922] A remote code execution vulnerability exists in the way that Microsoft COM for Windows handles objects in memory, aka 'Microsoft COM for Windows Remote Code Execution Vulnerability'.  
  
[CVE-2020-0938] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.  
  
[CVE-2020-0965] A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'.  
  
[CVE-2020-0982] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0987, CVE-2020-1005.  
  
[CVE-2020-0987] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-1005.  
  
[CVE-2020-1005] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-0987.  
  
[CVE-2020-1009] An elevation of privilege vulnerability exists in the way that the Microsoft Store Install Service handles file operations in protected locations, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-0983, CVE-2020-1011, CVE-2020-1015.  
  
[CVE-2020-1010] An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079.  
  
[CVE-2020-1013] An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates, aka 'Group Policy Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1014] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1018] An information disclosure vulnerability exists when Microsoft Dynamics Business Central/NAV on-premise does not properly hide the value of a masked field when showing the records as a chart page.The attacker who successfully exploited the vulnerability could see the information that are in a masked field.The security update addresses the vulnerability by updating the rendering engine the Windows client to properly detect masked fields and render the content as masked., aka 'Microsoft Dynamics Business Central/NAV Information Disclosure'.  
  
[CVE-2020-1020] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0938.  
  
[CVE-2020-1068] An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1079.  
  
[CVE-2020-1079] An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068.  
  
[CVE-2020-1083] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921.  
  
[CVE-2020-1118] A denial of service vulnerability exists in the Windows implementation of Transport Layer Security (TLS) when it improperly handles certain key exchanges, aka 'Microsoft Windows Transport Layer Security Denial of Service Vulnerability'.  
  
[CVE-2020-1129] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1319.  
  
[CVE-2020-1160] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-1163] An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170.  
  
[CVE-2020-1170] An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163.  
  
[CVE-2020-1206] An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.  
  
[CVE-2020-1243] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2020-1281] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2020-1284] A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'.  
  
[CVE-2020-1299] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-1300] A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'.  
  
[CVE-2020-1301] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'.  
  
[CVE-2020-13162] A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5.3 R70 for Windows (which runs as NT AUTHORITY/SYSTEM) allows unprivileged users to run a Microsoft Installer executable with elevated privileges.  
  
[CVE-2020-1319] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1129.  
  
[CVE-2020-1351] An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-1383] An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'.  
  
[CVE-2020-1408] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.  
  
[CVE-2020-1421] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-1425] A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1457.  
  
[CVE-2020-1457] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1425.  
  
[CVE-2020-1471] An elevation of privilege vulnerability exists when Microsoft Windows CloudExperienceHost fails to check COM objects, aka 'Windows CloudExperienceHost Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1507] An elevation of privilege vulnerability exists in the way that Microsoft COM for Windows handles objects in memory, aka 'Microsoft COM for Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-15145] In Composer-Setup for Windows before version 6.0.0, if the developer's computer is shared with other users, a local attacker may be able to exploit the following scenarios. 1. A local regular user may modify the existing `C:\ProgramData\ComposerSetup\bin\composer.bat` in order to get elevated command execution when composer is run by an administrator. 2. A local regular user may create a specially crafted dll in the `C:\ProgramData\ComposerSetup\bin` folder in order to get Local System privileges. See: https://itm4n.github.io/windows-server-netman-dll-hijacking. 3. If the directory of the php.exe selected by the user is not in the system path, it is added without checking that it is admin secured, as per Microsoft guidelines. See: https://msrc-blog.microsoft.com/2018/04/04/triaging-a-dll-planting-vulnerability.  
  
[CVE-2020-1560] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1574, CVE-2020-1585.  
  
[CVE-2020-1574] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1585.  
  
[CVE-2020-1585] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1574.  
  
[CVE-2020-16877] An elevation of privilege vulnerability exists when Microsoft Windows improperly handles reparse points, aka 'Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-16910] A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location.To exploit this vulnerability, an attacker could run a specially crafted application to bypass Unified Extensible Firmware Interface (UEFI) variable security in Windows.The security update addresses the vulnerability by correcting security feature behavior to enforce permissions., aka 'Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2020-17022] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'.  
  
[CVE-2020-17162] Microsoft Windows Security Feature Bypass Vulnerability  
  
[CVE-2020-24556] A vulnerability in Trend Micro Apex One, OfficeScan XG SP1, Worry-Free Business Security 10 SP1 and Worry-Free Business Security Services on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.  
  
[CVE-2020-24557] A vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.  
  
[CVE-2020-24562] A vulnerability in Trend Micro OfficeScan XG SP1 on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This CVE is similar, but not identical to CVE-2020-24556.  
  
[CVE-2020-25182] Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x searches for and loads DLLs as dynamic libraries. Uncontrolled loading of dynamic libraries could allow a local, unauthenticated attacker to execute arbitrary code. This vulnerability only affects ISaGRAF Runtime when running on Microsoft Windows systems.  
  
[CVE-2020-3127] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3128] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3194] A vulnerability in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3319] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.  
  
[CVE-2020-3321] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.  
  
[CVE-2020-3322] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.  
  
[CVE-2020-36233] The Microsoft Windows Installer for Atlassian Bitbucket Server and Data Center before version 6.10.9, 7.x before 7.6.4, and from version 7.7.0 before 7.10.1 allows local attackers to escalate privileges because of weak permissions on the installation directory.  
  
[CVE-2020-36603] The HoYoVerse (formerly miHoYo) Genshin Impact mhyprot2.sys 1.0.0.0 anti-cheat driver does not adequately restrict unprivileged function calls, allowing local, unprivileged users to execute arbitrary code with SYSTEM privileges on Microsoft Windows systems. The mhyprot2.sys driver must first be installed by a user with administrative privileges.  
  
[CVE-2020-4739] IBM DB2 Accessories Suite for Linux, UNIX, and Windows, DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 188149.  
  
[CVE-2020-4767] IBM Sterling Connect Direct for Microsoft Windows 4.7, 4.8, 6.0, and 6.1 could allow a remote attacker to cause a denial of service, caused by a buffer over-read. Bysending a specially crafted request, the attacker could cause the application to crash. IBM X-Force ID: 188906.  
  
[CVE-2020-5384] Authentication Bypass Vulnerability RSA MFA Agent 2.0 for Microsoft Windows contains an Authentication Bypass vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability by using an alternate path to bypass authentication in order to gain full access to the system.  
  
[CVE-2020-7205] "A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. \*\*Note:\*\* This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. \*\*Note:\*\* This DBX update mitigates the GRUB2 issue with insmod enabled, and the ""Boot Hole"" issue for HPE signed GRUB2 applications."  
  
[CVE-2020-7299] "Cleartext Storage of Sensitive Information in Memory vulnerability in Microsoft Windows client in McAfee True Key (TK) prior to 6.2.109.2 allows a local user logged in with administrative privileges to access to another user&#8217  
[CVE-2020-7320] Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing otherwise detected malware to run via stopping certain Microsoft services.  
  
[CVE-2020-7335] Privilege Escalation vulnerability in Microsoft Windows client McAfee Total Protection (MTP) prior to 16.0.29 allows local users to gain elevated privileges via careful manipulation of a folder by creating a junction link. This exploits a lack of protection through a timing issue and is only exploitable in a small time window.  
  
[CVE-2021-1372] A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens. Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.  
  
[CVE-2021-1710] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-21513] Dell EMC OpenManage Server Administrator (OMSA) version 9.5 Microsoft Windows installations with Distributed Web Server (DWS) enabled configuration contains an authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain admin access on the affected system.  
  
[CVE-2021-21706] In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.  
  
[CVE-2021-24076] Microsoft Windows VMSwitch Information Disclosure Vulnerability  
  
[CVE-2021-24081] Microsoft Windows Codecs Library Remote Code Execution Vulnerability  
  
[CVE-2021-26432] Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability  
  
[CVE-2021-26433] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-36926, CVE-2021-36932, CVE-2021-36933.  
  
[CVE-2021-26881] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-26887] Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability  
  
[CVE-2021-28317] Microsoft Windows Codecs Library Information Disclosure Vulnerability  
  
[CVE-2021-31184] Microsoft Windows Infrared Data Association (IrDA) Information Disclosure Vulnerability  
  
[CVE-2021-32022] A low privileged delete vulnerability using CEF RPC server of BlackBerry Protect for Windows version(s) versions 1574 and earlier could allow an attacker to potentially execute code in the context of a BlackBerry Cylance service that has admin rights on the system and gaining the ability to delete data from the local system.  
  
[CVE-2021-34439] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34441, CVE-2021-34503.  
  
[CVE-2021-34441] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34503.  
  
[CVE-2021-34471] Microsoft Windows Defender Elevation of Privilege Vulnerability  
  
[CVE-2021-34503] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34441.  
  
[CVE-2021-34579] "In Phoenix Contact: FL MGUARD DM version 1.12.0 and 1.13.0 access to the Apache web server being installed as part of the FL MGUARD DM on Microsoft Windows does not require login credentials even if configured during installation.Attackers with network access to the Apache web server can download and therefore read mGuard configuration profiles (&#8220  
[CVE-2021-35211] Microsoft discovered a remote code execution (RCE) vulnerability in the SolarWinds Serv-U product utilizing a Remote Memory Escape Vulnerability. If exploited, a threat actor may be able to gain privileged access to the machine hosting Serv-U Only. SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows before 15.2.3 HF2 are affected by this vulnerability.  
  
[CVE-2021-36745] A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass authentication on affected installations.  
  
[CVE-2021-36926] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36932, CVE-2021-36933.  
  
[CVE-2021-36932] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36926, CVE-2021-36933.  
  
[CVE-2021-36933] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36926, CVE-2021-36932.  
  
[CVE-2021-38505] "Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats  
[CVE-2021-38634] Microsoft Windows Update Client Elevation of Privilege Vulnerability  
  
[CVE-2021-39032] IBM Sterling Gentran:Server for Microsoft Windows 5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 213962.  
  
[CVE-2021-40828] Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.3.3), Python (versions prior to 1.5.18), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.1) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on Windows. This issue has been addressed in aws-c-io submodule versions 0.9.13 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.3.3 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.5.18 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on Microsoft Windows.  
  
[CVE-2021-41065] An issue was discovered in Listary through 6. An attacker can create a \\.\pipe\Listary.listaryService named pipe and wait for a privileged user to open a session on the Listary installed host. Listary will automatically access the named pipe and the attacker will be able to duplicate the victim's token to impersonate him. This exploit is valid in certain Windows versions (Microsoft has patched the issue in later Windows 10 builds).  
  
[CVE-2021-41330] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-42275] Microsoft COM for Windows Remote Code Execution Vulnerability  
  
[CVE-2021-42276] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2022-1794] The CODESYS OPC DA Server prior V3.5.18.20 stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system.  
  
[CVE-2022-21606] Vulnerability in the Oracle Services for Microsoft Transaction Server component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Services for Microsoft Transaction Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Services for Microsoft Transaction Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Services for Microsoft Transaction Server accessible data as well as unauthorized read access to a subset of Oracle Services for Microsoft Transaction Server accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).  
  
[CVE-2022-21993] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability  
  
[CVE-2022-22516] The SysDrv3S driver in the CODESYS Control runtime system on Microsoft Windows allows any system user to read and write within restricted memory space.  
  
[CVE-2022-22765] BD Viper LT system, versions 2.0 and later, contains hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). BD Viper LT system versions 4.0 and later utilize Microsoft Windows 10 and have additional Operating System hardening configurations which increase the attack complexity required to exploit this vulnerability.  
  
[CVE-2022-22782] "The Zoom Client for Meetings for Windows prior to version 5.9.7, Zoom Rooms for Conference Room for Windows prior to version 5.10.0, Zoom Plugins for Microsoft Outlook for Windows prior to version 5.10.3, and Zoom VDI Windows Meeting Clients prior to version 5.9.6  
[CVE-2022-23235] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.10P1 are susceptible to a vulnerability which could allow an attacker to discover cluster, node and Active IQ Unified Manager specific information via AutoSupport telemetry data that is sent even when AutoSupport has been disabled.  
  
[CVE-2022-23239] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows administrative users to perform a Stored Cross-Site Scripting (XSS) attack.  
  
[CVE-2022-23240] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows unauthorized users to update EMS Subscriptions via unspecified vectors.  
  
[CVE-2022-23609] iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible.  
  
[CVE-2022-23611] iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdcd48b. Users are advised to upgrade.  
  
[CVE-2022-23678] A vulnerability in the Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system client communications that could allow for an attacker in a privileged network position to intercept sensitive information in Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system versions: 4.3.0 build 2208101 and below. Aruba has released upgrades for Virtual Intranet Access (VIA) Client that address this security vulnerability.  
  
[CVE-2022-24765] Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder `C:\.git`, which would be picked up by Git operations run supposedly outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash users who set `GIT\_PS1\_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-gitare vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config`. Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access from those folders as a workaround. Alternatively, define or extend `GIT\_CEILING\_DIRECTORIES` to cover the \_parent\_ directory of the user profile, e.g. `C:\Users` if the user profile is located in `C:\Users\my-user-name`.  
  
[CVE-2022-24826] On Windows, if Git LFS operates on a malicious repository with a `..exe` file as well as a file named `git.exe`, and `git.exe` is not found in `PATH`, the `..exe` program will be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. Similarly, if the malicious repository contains files named `..exe` and `cygpath.exe`, and `cygpath.exe` is not found in `PATH`, the `..exe` program will be executed when certain Git LFS commands are run. More generally, if the current working directory contains any file with a base name of `.` and a file extension from `PATHEXT` (except `.bat` and `.cmd`), and also contains another file with the same base name as a program Git LFS intends to execute (such as `git`, `cygpath`, or `uname`) and any file extension from `PATHEXT` (including `.bat` and `.cmd`), then, on Windows, when Git LFS attempts to execute the intended program the `..exe`, `..com`, etc., file will be executed instead, but only if the intended program is not found in any directory listed in `PATH`. The vulnerability occurs because when Git LFS detects that the program it intends to run does not exist in any directory listed in `PATH` then Git LFS passes an empty string as the executable file path to the Go `os/exec` package, which contains a bug such that, on Windows, it prepends the name of the current working directory (i.e., `.`) to the empty string without adding a path separator, and as a result searches in that directory for a file with the base name `.` combined with any file extension from `PATHEXT`, executing the first one it finds. (The reason `..bat` and `..cmd` files are not executed in the same manner is that, although the Go `os/exec` package tries to execute them just as it does a `..exe` file, the Microsoft Win32 API `CreateProcess()` family of functions have an undocumented feature in that they apparently recognize when a caller is attempting to execute a batch script file and instead run the `cmd.exe` command interpreter, passing the full set of command line arguments as parameters. These are unchanged from the command line arguments set by Git LFS, and as such, the intended program's name is the first, resulting in a command line like `cmd.exe /c git`, which then fails.) Git LFS has resolved this vulnerability by always reporting an error when a program is not found in any directory listed in `PATH` rather than passing an empty string to the Go `os/exec` package in this case. The bug in the Go `os/exec` package has been reported to the Go project and is expected to be patched after this security advisory is published. The problem was introduced in version 2.12.1 and is patched in version 3.1.3. Users of affected versions should upgrade to version 3.1.3. There are currently no known workarounds at this time.  
  
[CVE-2022-27167] "Privilege escalation vulnerability in Windows products of ESET, spol. s r.o. allows attacker to exploit ""Repair"" and ""Uninstall"" features what may lead to arbitrary file deletion. This issue affects: ESET, spol. s r.o. ESET NOD32 Antivirus 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Internet Security 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Smart Security Premium 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Endpoint Antivirus 6.0 versions prior to 9.0.2046.0. ESET, spol. s r.o. ESET Endpoint Security 6.0 versions prior to 9.0.2046.0. ESET, spol. s r.o. ESET Server Security for Microsoft Windows Server 8.0 versions prior to 9.0.12012.0. ESET, spol. s r.o. ESET File Security for Microsoft Windows Server 8.0.12013.0. ESET, spol. s r.o. ESET Mail Security for Microsoft Exchange Server 6.0 versions prior to 8.0.10020.0. ESET, spol. s r.o. ESET Mail Security for IBM Domino 6.0 versions prior to 8.0.14011.0. ESET, spol. s r.o. ESET Security for Microsoft SharePoint Server 6.0 versions prior to 8.0.15009.0."  
  
[CVE-2022-27608] Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows is vulnerable to registry key tampering by users with Administrator privileges. This could result in a user disabling anti-tampering mechanisms which would then allow the user to disable Forcepoint One Endpoint and the protection offered by it.  
  
[CVE-2022-27609] Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling Forcepoint One Endpoint and the protection offered by it.  
  
[CVE-2022-29105] Microsoft Windows Media Foundation Remote Code Execution Vulnerability.  
  
[CVE-2022-30190] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.  
  
[CVE-2022-32230] Microsoft Windows SMBv3 suffers from a null pointer dereference in versions of Windows prior to the April, 2022 patch set. By sending a malformed FileNormalizedNameInformation SMBv3 request over a named pipe, an attacker can cause a Blue Screen of Death (BSOD) crash of the Windows kernel. For most systems, this attack requires authentication, except in the special case of Windows Domain Controllers, where unauthenticated users can always open named pipes as long as they can establish an SMB session. Typically, after the BSOD, the victim SMBv3 server will reboot.  
  
[CVE-2022-34006] An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. When installing, Microsoft SQL Express 2019 installs by default with an SQL instance running as SYSTEM with BUILTIN\Users as sysadmin, thus enabling unprivileged Windows users to execute commands locally as NT AUTHORITY\SYSTEM, aka NX-I674 (sub-issue 2). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation.  
  
[CVE-2022-34478] The <code>ms-msdt</code>, <code>search</code>, and <code>search-ms</code> protocols deliver content to Microsoft applications, bypassing the browser, when a user accepts a prompt. These applications have had known vulnerabilities, exploited in the wild (although we know of none exploited through Thunderbird), so in this release Thunderbird has blocked these protocols from prompting the user to open them.<br>\*This bug only affects Thunderbird on Windows. Other operating systems are unaffected.\*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.  
  
[CVE-2022-34713] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability  
  
[CVE-2022-35743] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability  
  
[CVE-2022-36670] PCProtect Endpoint prior to v5.17.470 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.  
  
[CVE-2022-37771] IObit Malware Fighter v9.2 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.  
  
[CVE-2022-37971] Microsoft Windows Defender Elevation of Privilege Vulnerability.  
  
[CVE-2022-39327] Azure CLI is the command-line interface for Microsoft Azure. In versions previous to 2.40.0, Azure CLI contains a vulnerability for potential code injection. Critical scenarios are where a hosting machine runs an Azure CLI command where parameter values have been provided by an external source. The vulnerability is only applicable when the Azure CLI command is run on a Windows machine and with any version of PowerShell and when the parameter value contains the `&` or `|` symbols. If any of these prerequisites are not met, this vulnerability is not applicable. Users should upgrade to version 2.40.0 or greater to receive a a mitigation for the vulnerability.  
  
[CVE-2022-40263] BD Totalys MultiProcessor, versions 1.70 and earlier, contain hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). Customers using BD Totalys MultiProcessor version 1.70 with Microsoft Windows 10 have additional operating system hardening configurations which increase the attack complexity required to exploit this vulnerability.  
  
[CVE-2022-41120] Microsoft Windows System Monitor (Sysmon) Elevation of Privilege Vulnerability  
  
[CVE-2022-44704] Microsoft Windows Sysmon Elevation of Privilege Vulnerability.  
  
[CVE-2022-45141] Since the Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96).  
  
[CVE-2023-1587] Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The issue was fixed with Avast and AVG Antivirus version 22.11  
  
[CVE-2023-22880] "Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft&#8217  
[CVE-2023-28005] "A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows&#65533  
[CVE-2023-28290] Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability  
  
[CVE-2023-28297] Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability  
  
[CVE-2023-31222] "Deserialization of untrusted data in Microsoft Messaging Queuing Service in Medtronic's Paceart Optima versions 1.11 and earlier on Windows allows an unauthorized user to impact a healthcare delivery organization&#8217  
[CVE-2023-34355] Uncontrolled search path element for some Intel(R) Server Board M10JNP2SB integrated BMC video drivers before version 3.0 for Microsoft Windows and before version 1.13.4 for linux may allow an authenticated user to potentially enable escalation of privilege via local access.  
  
[CVE-2023-38175] Microsoft Windows Defender Elevation of Privilege Vulnerability  
  
[CVE-2023-38402] A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow malicious users to overwrite arbitrary files as NT AUTHORITY\SYSTEM. A successful exploit could allow these malicious users to create a Denial-of-Service (DoS) condition affecting the Microsoft Windows operating System boot process.

### Узел 192.168.233.1/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 3368

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 135 | open | syn-ack | msrpc | [CVE-2000-0771] - Информация неизвестна [CVE-2001-0509] - Информация неизвестна [CVE-2002-1140] - Средняя [CVE-2002-1141] - Средняя [CVE-2003-0003] - Высокая [CVE-2003-0352] - Высокая [CVE-2003-0807] - Средняя [CVE-2004-0116] - Средняя [CVE-2004-0124] - Низкая [CVE-2004-0569] - Высокая [CVE-2005-3644] - Высокая [CVE-2006-0013] - Средняя [CVE-2006-0034] - Высокая [CVE-2006-2370] - Высокая [CVE-2006-2371] - Высокая [CVE-2006-2380] - Средняя [CVE-2006-3439] - Критичная [CVE-2006-4691] - Критичная [CVE-2006-6296] - Средняя [CVE-2006-6723] - Высокая [CVE-2007-1748] - Критичная [CVE-2007-2228] - Высокая [CVE-2007-3039] - Критичная [CVE-2008-3479] - Критичная [CVE-2008-4114] - Высокая [CVE-2008-4250] - Критичная [CVE-2009-0079] - Средняя [CVE-2009-0228] - Критичная [CVE-2009-0230] - Критичная [CVE-2009-0568] - Критичная [CVE-2009-1544] - Критичная [CVE-2009-2523] - Критичная [CVE-2010-2567] - Критичная [CVE-2010-2729] - Критичная [CVE-2010-2742] - Средняя [CVE-2010-3139] - Критичная [CVE-2010-3222] - Высокая [CVE-2013-3175] - Критичная [CVE-2013-3878] - Средняя [CVE-2014-0316] - Высокая [CVE-2015-2370] - Высокая [CVE-2016-0128] - Средняя [CVE-2016-0178] - Высокая [CVE-2020-1113] - Высокая [CVE-1999-0012] - Информация неизвестна [CVE-1999-0227] - Информация неизвестна [CVE-1999-0228] - Информация неизвестна [CVE-1999-0288] - Информация неизвестна [CVE-1999-0386] - Информация неизвестна [CVE-1999-0681] - Информация неизвестна [CVE-1999-0749] - Информация неизвестна [CVE-1999-0969] - Информация неизвестна [CVE-1999-1127] - Информация неизвестна [CVE-1999-1291] - Информация неизвестна [CVE-2000-0089] - Информация неизвестна [CVE-2000-0168] - Информация неизвестна [CVE-2000-0216] - Информация неизвестна [CVE-2000-0228] - Информация неизвестна [CVE-2000-0331] - Информация неизвестна [CVE-2000-0495] - Информация неизвестна [CVE-2000-0544] - Информация неизвестна [CVE-2000-0653] - Информация неизвестна [CVE-2000-0742] - Информация неизвестна [CVE-2000-0790] - Информация неизвестна [CVE-2000-0849] - Информация неизвестна [CVE-2000-0858] - Информация неизвестна [CVE-2000-0929] - Информация неизвестна [CVE-2000-0942] - Информация неизвестна [CVE-2000-1079] - Информация неизвестна [CVE-2000-1112] - Информация неизвестна [CVE-2000-1113] - Информация неизвестна [CVE-2000-1217] - Информация неизвестна [CVE-2000-1218] - Информация неизвестна [CVE-2001-0003] - Информация неизвестна [CVE-2001-0047] - Информация неизвестна [CVE-2001-0242] - Информация неизвестна [CVE-2001-0245] - Информация неизвестна [CVE-2001-0261] - Информация неизвестна [CVE-2001-0345] - Информация неизвестна [CVE-2001-0346] - Информация неизвестна [CVE-2001-0347] - Информация неизвестна [CVE-2001-0348] - Информация неизвестна [CVE-2001-0349] - Информация неизвестна [CVE-2001-0350] - Информация неизвестна [CVE-2001-0351] - Информация неизвестна [CVE-2001-0504] - Информация неизвестна [CVE-2001-0541] - Информация неизвестна [CVE-2001-0662] - Информация неизвестна [CVE-2001-0719] - Информация неизвестна [CVE-2001-0909] - Информация неизвестна [CVE-2001-1055] - Информация неизвестна [CVE-2001-1200] - Информация неизвестна [CVE-2001-1451] - Информация неизвестна [CVE-2002-0018] - Критичная [CVE-2002-0034] - Средняя [CVE-2002-0054] - Высокая [CVE-2002-0055] - Средняя [CVE-2002-0136] - Средняя [CVE-2002-0151] - Высокая [CVE-2002-0224] - Средняя [CVE-2002-0370] - Высокая [CVE-2002-0372] - Высокая [CVE-2002-0373] - Высокая [CVE-2002-0443] - Средняя [CVE-2002-0444] - Высокая [CVE-2002-0597] - Средняя [CVE-2002-0615] - Высокая [CVE-2002-0616] - Средняя [CVE-2002-0617] - Средняя [CVE-2002-0618] - Высокая [CVE-2002-0619] - Высокая [CVE-2002-0693] - Высокая [CVE-2002-0694] - Высокая [CVE-2002-0699] - Средняя [CVE-2002-0724] - Высокая [CVE-2002-0862] - Высокая [CVE-2002-0863] - Средняя [CVE-2002-0864] - Средняя [CVE-2002-1139] - Средняя [CVE-2002-1183] - Высокая [CVE-2002-1184] - Средняя [CVE-2002-1214] - Высокая [CVE-2002-1256] - Средняя [CVE-2002-1327] - Высокая [CVE-2002-1561] - Средняя [CVE-2002-1670] - Средняя [CVE-2002-1692] - Низкая [CVE-2002-1712] - Средняя [CVE-2002-1844] - Высокая [CVE-2002-1847] - Высокая [CVE-2002-1873] - Средняя [CVE-2002-1932] - Высокая [CVE-2002-1933] - Высокая [CVE-2002-1984] - Средняя [CVE-2002-2073] - Средняя [CVE-2002-2105] - Низкая [CVE-2002-2117] - Средняя [CVE-2002-2283] - Низкая [CVE-2003-0004] - Высокая [CVE-2003-0009] - Средняя [CVE-2003-0109] - Высокая [CVE-2003-0111] - Высокая [CVE-2003-0227] - Средняя [CVE-2003-0228] - Высокая [CVE-2003-0345] - Высокая [CVE-2003-0346] - Высокая [CVE-2003-0348] - Средняя [CVE-2003-0349] - Высокая [CVE-2003-0496] - Высокая [CVE-2003-0533] - Высокая [CVE-2003-0604] - Высокая [CVE-2003-0605] - Высокая [CVE-2003-0660] - Высокая [CVE-2003-0662] - Критичная [CVE-2003-0719] - Высокая [CVE-2003-0806] - Высокая [CVE-2003-0812] - Высокая [CVE-2003-0813] - Средняя [CVE-2003-0818] - Высокая [CVE-2003-0825] - Критичная [CVE-2003-0839] - Средняя [CVE-2003-0906] - Высокая [CVE-2003-0907] - Средняя [CVE-2003-0908] - Высокая [CVE-2003-0995] - Высокая [CVE-2003-1106] - Средняя [CVE-2003-1107] - Средняя [CVE-2004-0120] - Средняя [CVE-2004-0199] - Средняя [CVE-2004-0201] - Критичная [CVE-2004-0202] - Средняя [CVE-2004-0206] - Высокая [CVE-2004-0207] - Низкая [CVE-2004-0208] - Высокая [CVE-2004-0209] - Критичная [CVE-2004-0210] - Высокая [CVE-2004-0211] - Низкая [CVE-2004-0214] - Критичная [CVE-2004-0503] - Средняя [CVE-2004-0540] - Критичная [CVE-2004-0571] - Критичная [CVE-2004-0572] - Критичная [CVE-2004-0574] - Критичная [CVE-2004-0575] - Критичная [CVE-2004-0726] - Высокая [CVE-2004-0727] - Высокая [CVE-2004-0840] - Критичная [CVE-2004-0897] - Критичная [CVE-2004-0899] - Средняя [CVE-2004-0900] - Критичная [CVE-2004-0901] - Критичная [CVE-2004-1049] - Средняя [CVE-2004-1080] - Критичная [CVE-2004-1324] - Низкая [CVE-2004-1325] - Средняя [CVE-2004-1889] - Средняя [CVE-2004-2176] - Средняя [CVE-2004-2289] - Критичная [CVE-2004-2290] - Высокая [CVE-2004-2291] - Высокая [CVE-2004-2307] - Средняя [CVE-2004-2339] - Высокая [CVE-2004-2365] - Низкая [CVE-2004-2454] - Низкая [CVE-2004-2527] - Средняя [CVE-2005-0048] - Высокая [CVE-2005-0058] - Высокая [CVE-2005-0059] - Критичная [CVE-2005-0060] - Высокая [CVE-2005-0061] - Высокая [CVE-2005-0063] - Высокая [CVE-2005-0545] - Высокая [CVE-2005-0550] - Низкая [CVE-2005-0551] - Критичная [CVE-2005-0771] - Критичная [CVE-2005-0852] - Низкая [CVE-2005-1205] - Средняя [CVE-2005-1206] - Высокая [CVE-2005-1207] - Высокая [CVE-2005-1208] - Критичная [CVE-2005-1218] - Средняя [CVE-2005-1219] - Высокая [CVE-2005-1792] - Средняя [CVE-2005-1793] - Низкая [CVE-2005-1978] - Высокая [CVE-2005-1979] - Средняя [CVE-2005-1980] - Средняя [CVE-2005-1981] - Низкая [CVE-2005-1982] - Низкая [CVE-2005-1983] - Критичная [CVE-2005-1984] - Высокая [CVE-2005-1985] - Высокая [CVE-2005-1987] - Высокая [CVE-2005-2117] - Средняя [CVE-2005-2118] - Средняя [CVE-2005-2120] - Средняя [CVE-2005-2122] - Критичная [CVE-2005-2128] - Средняя [CVE-2005-2224] - Средняя [CVE-2005-2307] - Средняя [CVE-2005-2388] - Высокая [CVE-2005-2935] - Средняя [CVE-2005-2940] - Высокая [CVE-2005-3168] - Высокая [CVE-2005-3169] - Средняя [CVE-2005-3170] - Средняя [CVE-2005-3171] - Средняя [CVE-2005-3172] - Средняя [CVE-2005-3173] - Средняя [CVE-2005-3174] - Средняя [CVE-2005-3175] - Высокая [CVE-2005-3176] - Высокая [CVE-2005-3177] - Средняя [CVE-2005-3595] - Критичная [CVE-2005-3945] - Высокая [CVE-2005-3981] - Средняя [CVE-2005-4269] - Высокая [CVE-2005-4360] - Высокая [CVE-2005-4560] - Высокая [CVE-2005-4717] - Средняя [CVE-2006-0005] - Критичная [CVE-2006-0006] - Критичная [CVE-2006-0008] - Высокая [CVE-2006-0010] - Критичная [CVE-2006-0012] - Средняя [CVE-2006-0014] - Средняя [CVE-2006-0020] - Критичная [CVE-2006-0021] - Высокая [CVE-2006-0023] - Средняя [CVE-2006-0025] - Критичная [CVE-2006-0032] - Средняя [CVE-2006-0143] - Высокая [CVE-2006-0561] - Высокая [CVE-2006-0753] - Низкая [CVE-2006-0988] - Высокая [CVE-2006-1184] - Средняя [CVE-2006-1300] - Средняя [CVE-2006-1311] - Критичная [CVE-2006-1313] - Средняя [CVE-2006-1314] - Высокая [CVE-2006-1315] - Средняя [CVE-2006-1475] - Низкая [CVE-2006-1476] - Низкая [CVE-2006-1510] - Средняя [CVE-2006-1591] - Средняя [CVE-2006-1651] - Высокая [CVE-2006-1654] - Средняя [CVE-2006-2056] - Средняя [CVE-2006-2094] - Средняя [CVE-2006-2218] - Критичная [CVE-2006-2334] - Низкая [CVE-2006-2372] - Критичная [CVE-2006-2373] - Критичная [CVE-2006-2374] - Низкая [CVE-2006-2376] - Высокая [CVE-2006-2378] - Средняя [CVE-2006-2379] - Критичная [CVE-2006-2386] - Средняя [CVE-2006-2766] - Низкая [CVE-2006-3209] - Высокая [CVE-2006-3440] - Критичная [CVE-2006-3441] - Критичная [CVE-2006-3442] - Высокая [CVE-2006-3443] - Высокая [CVE-2006-3444] - Высокая [CVE-2006-3445] - Высокая [CVE-2006-3448] - Критичная [CVE-2006-3471] - Средняя [CVE-2006-3510] - Низкая [CVE-2006-3643] - Средняя [CVE-2006-3648] - Высокая [CVE-2006-3730] - Критичная [CVE-2006-3869] - Высокая [CVE-2006-3873] - Высокая [CVE-2006-3880] - Средняя [CVE-2006-3897] - Средняя [CVE-2006-3898] - Средняя [CVE-2006-3899] - Средняя [CVE-2006-3915] - Средняя [CVE-2006-3942] - Высокая [CVE-2006-3943] - Низкая [CVE-2006-3944] - Средняя [CVE-2006-3992] - Средняя [CVE-2006-4066] - Низкая [CVE-2006-4071] - Низкая [CVE-2006-4128] - Средняя [CVE-2006-4138] - Высокая [CVE-2006-4219] - Высокая [CVE-2006-4495] - Высокая [CVE-2006-4688] - Высокая [CVE-2006-4689] - Средняя [CVE-2006-4692] - Средняя [CVE-2006-4694] - Критичная [CVE-2006-4696] - Критичная [CVE-2006-4702] - Средняя [CVE-2006-4868] - Критичная [CVE-2006-5028] - Средняя [CVE-2006-5270] - Критичная [CVE-2006-5448] - Высокая [CVE-2006-5583] - Критичная [CVE-2006-5584] - Высокая [CVE-2006-5585] - Высокая [CVE-2006-5586] - Высокая [CVE-2006-5614] - Низкая [CVE-2006-5745] - Высокая [CVE-2006-5758] - Высокая [CVE-2006-6134] - Высокая [CVE-2006-6252] - Средняя [CVE-2006-6579] - Средняя [CVE-2006-6601] - Средняя [CVE-2006-6602] - Средняя [CVE-2006-6659] - Средняя [CVE-2006-6696] - Средняя [CVE-2006-6753] - Средняя [CVE-2006-6797] - Средняя [CVE-2006-6901] - Критичная [CVE-2006-6902] - Критичная [CVE-2006-7066] - Высокая [CVE-2006-7206] - Высокая [CVE-2006-7210] - Средняя [CVE-2007-0024] - Критичная [CVE-2007-0025] - Критичная [CVE-2007-0026] - Высокая [CVE-2007-0038] - Критичная [CVE-2007-0040] - Критичная [CVE-2007-0041] - Критичная [CVE-2007-0042] - Высокая [CVE-2007-0043] - Критичная [CVE-2007-0045] - Средняя [CVE-2007-0064] - Критичная [CVE-2007-0065] - Критичная [CVE-2007-0066] - Высокая [CVE-2007-0069] - Критичная [CVE-2007-0084] - Средняя [CVE-2007-0210] - Высокая [CVE-2007-0211] - Высокая [CVE-2007-0214] - Критичная [CVE-2007-0351] - Средняя [CVE-2007-0562] - Средняя [CVE-2007-0612] - Высокая [CVE-2007-0675] - Высокая [CVE-2007-0811] - Средняя [CVE-2007-0843] - Средняя [CVE-2007-0878] - Высокая [CVE-2007-0942] - Критичная [CVE-2007-0944] - Критичная [CVE-2007-0945] - Критичная [CVE-2007-0946] - Критичная [CVE-2007-0947] - Критичная [CVE-2007-1070] - Критичная [CVE-2007-1090] - Высокая [CVE-2007-1204] - Средняя [CVE-2007-1205] - Критичная [CVE-2007-1206] - Высокая [CVE-2007-1209] - Высокая [CVE-2007-1211] - Высокая [CVE-2007-1212] - Средняя [CVE-2007-1213] - Высокая [CVE-2007-1215] - Высокая [CVE-2007-1347] - Высокая [CVE-2007-1492] - Высокая [CVE-2007-1499] - Средняя [CVE-2007-1512] - Критичная [CVE-2007-1527] - Средняя [CVE-2007-1528] - Средняя [CVE-2007-1529] - Средняя [CVE-2007-1530] - Средняя [CVE-2007-1531] - Средняя [CVE-2007-1532] - Средняя [CVE-2007-1533] - Средняя [CVE-2007-1534] - Критичная [CVE-2007-1535] - Высокая [CVE-2007-1537] - Низкая [CVE-2007-1644] - Критичная [CVE-2007-1645] - Критичная [CVE-2007-1658] - Критичная [CVE-2007-1692] - Высокая [CVE-2007-1763] - Высокая [CVE-2007-1765] - Критичная [CVE-2007-1912] - Средняя [CVE-2007-1946] - Критичная [CVE-2007-1973] - Средняя [CVE-2007-2217] - Критичная [CVE-2007-2218] - Критичная [CVE-2007-2219] - Критичная [CVE-2007-2221] - Критичная [CVE-2007-2224] - Критичная [CVE-2007-2225] - Средняя [CVE-2007-2227] - Средняя [CVE-2007-2229] - Высокая [CVE-2007-2237] - Высокая [CVE-2007-2374] - Критичная [CVE-2007-2528] - Критичная [CVE-2007-2581] - Средняя [CVE-2007-2593] - Высокая [CVE-2007-2729] - Высокая [CVE-2007-2730] - Высокая [CVE-2007-2815] - Критичная [CVE-2007-2954] - Критичная [CVE-2007-2966] - Высокая [CVE-2007-2967] - Критичная [CVE-2007-2999] - Низкая [CVE-2007-3028] - Средняя [CVE-2007-3034] - Критичная [CVE-2007-3035] - Высокая [CVE-2007-3036] - Средняя [CVE-2007-3037] - Средняя [CVE-2007-3038] - Высокая [CVE-2007-3040] - Критичная [CVE-2007-3300] - Критичная [CVE-2007-3406] - Средняя [CVE-2007-3436] - Средняя [CVE-2007-3463] - Средняя [CVE-2007-3509] - Высокая [CVE-2007-3671] - Высокая [CVE-2007-3724] - Низкая [CVE-2007-3826] - Критичная [CVE-2007-3896] - Критичная [CVE-2007-3897] - Критичная [CVE-2007-3898] - Средняя [CVE-2007-3958] - Высокая [CVE-2007-4218] - Критичная [CVE-2007-4219] - Критичная [CVE-2007-4227] - Средняя [CVE-2007-4247] - Средняя [CVE-2007-4288] - Средняя [CVE-2007-4414] - Средняя [CVE-2007-4490] - Критичная [CVE-2007-5095] - Высокая [CVE-2007-5133] - Высокая [CVE-2007-5145] - Средняя [CVE-2007-5348] - Критичная [CVE-2007-5350] - Высокая [CVE-2007-5351] - Критичная [CVE-2007-5352] - Высокая [CVE-2007-5460] - Высокая [CVE-2007-5587] - Средняя [CVE-2007-5633] - Высокая [CVE-2007-5634] - Средняя [CVE-2007-6043] - Высокая [CVE-2007-6236] - Средняя [CVE-2007-6332] - Критичная [CVE-2007-6401] - Критичная [CVE-2007-6507] - Критичная [CVE-2007-6701] - Критичная [CVE-2007-6753] - Средняя [CVE-2008-0015] - Критичная [CVE-2008-0020] - Критичная [CVE-2008-0080] - Критичная [CVE-2008-0083] - Критичная [CVE-2008-0084] - Высокая [CVE-2008-0087] - Высокая [CVE-2008-0088] - Средняя [CVE-2008-0322] - Высокая [CVE-2008-0639] - Критичная [CVE-2008-0768] - Критичная [CVE-2008-0951] - Критичная [CVE-2008-1083] - Критичная [CVE-2008-1084] - Высокая [CVE-2008-1086] - Критичная [CVE-2008-1087] - Критичная [CVE-2008-1435] - Критичная [CVE-2008-1436] - Критичная [CVE-2008-1440] - Высокая [CVE-2008-1441] - Средняя [CVE-2008-1444] - Критичная [CVE-2008-1445] - Высокая [CVE-2008-1446] - Критичная [CVE-2008-1448] - Высокая [CVE-2008-1451] - Высокая [CVE-2008-1453] - Высокая [CVE-2008-1454] - Критичная [CVE-2008-1456] - Критичная [CVE-2008-1457] - Критичная [CVE-2008-1888] - Средняя [CVE-2008-2160] - Критичная [CVE-2008-2245] - Критичная [CVE-2008-2246] - Высокая [CVE-2008-2249] - Критичная [CVE-2008-2250] - Высокая [CVE-2008-2251] - Высокая [CVE-2008-2252] - Высокая [CVE-2008-2253] - Критичная [CVE-2008-2540] - Критичная [CVE-2008-2547] - Критичная [CVE-2008-3008] - Критичная [CVE-2008-3009] - Критичная [CVE-2008-3010] - Критичная [CVE-2008-3012] - Критичная [CVE-2008-3013] - Критичная [CVE-2008-3014] - Критичная [CVE-2008-3068] - Высокая [CVE-2008-3464] - Высокая [CVE-2008-3465] - Критичная [CVE-2008-3466] - Критичная [CVE-2008-3636] - Высокая [CVE-2008-3648] - Критичная [CVE-2008-3815] - Средняя [CVE-2008-3893] - Низкая [CVE-2008-3957] - Критичная [CVE-2008-4023] - Критичная [CVE-2008-4036] - Высокая [CVE-2008-4037] - Критичная [CVE-2008-4038] - Критичная [CVE-2008-4071] - Средняя [CVE-2008-4127] - Средняя [CVE-2008-4255] - Критичная [CVE-2008-4261] - Критичная [CVE-2008-4268] - Высокая [CVE-2008-4269] - Высокая [CVE-2008-4295] - Средняя [CVE-2008-4323] - Средняя [CVE-2008-4327] - Средняя [CVE-2008-4510] - Средняя [CVE-2008-4609] - Высокая [CVE-2008-4834] - Критичная [CVE-2008-4835] - Критичная [CVE-2008-4841] - Критичная [CVE-2008-4927] - Средняя [CVE-2008-5044] - Средняя [CVE-2008-5112] - Средняя [CVE-2008-5179] - Средняя [CVE-2008-5229] - Средняя [CVE-2008-5232] - Критичная [CVE-2008-5415] - Критичная [CVE-2008-5745] - Средняя [CVE-2008-5750] - Средняя [CVE-2008-5823] - Средняя [CVE-2008-5828] - Средняя [CVE-2008-6194] - Высокая [CVE-2008-6219] - Высокая [CVE-2008-6819] - Средняя [CVE-2009-0078] - Высокая [CVE-2009-0081] - Критичная [CVE-2009-0082] - Высокая [CVE-2009-0083] - Высокая [CVE-2009-0085] - Высокая [CVE-2009-0086] - Критичная [CVE-2009-0087] - Критичная [CVE-2009-0089] - Средняя [CVE-2009-0093] - Низкая [CVE-2009-0094] - Средняя [CVE-2009-0119] - Критичная [CVE-2009-0202] - Критичная [CVE-2009-0229] - Средняя [CVE-2009-0231] - Критичная [CVE-2009-0232] - Критичная [CVE-2009-0233] - Средняя [CVE-2009-0234] - Средняя [CVE-2009-0235] - Критичная [CVE-2009-0239] - Средняя [CVE-2009-0243] - Высокая [CVE-2009-0244] - Высокая [CVE-2009-0320] - Средняя [CVE-2009-0341] - Критичная [CVE-2009-0550] - Критичная [CVE-2009-0551] - Критичная [CVE-2009-0552] - Критичная [CVE-2009-0553] - Критичная [CVE-2009-0554] - Критичная [CVE-2009-0555] - Критичная [CVE-2009-1043] - Критичная [CVE-2009-1122] - Высокая [CVE-2009-1123] - Высокая [CVE-2009-1124] - Высокая [CVE-2009-1125] - Высокая [CVE-2009-1126] - Высокая [CVE-2009-1127] - Высокая [CVE-2009-1132] - Критичная [CVE-2009-1133] - Критичная [CVE-2009-1138] - Критичная [CVE-2009-1139] - Высокая [CVE-2009-1141] - Критичная [CVE-2009-1216] - Критичная [CVE-2009-1217] - Средняя [CVE-2009-1331] - Критичная [CVE-2009-1335] - Средняя [CVE-2009-1511] - Высокая [CVE-2009-1528] - Критичная [CVE-2009-1529] - Критичная [CVE-2009-1530] - Критичная [CVE-2009-1531] - Критичная [CVE-2009-1532] - Критичная [CVE-2009-1533] - Критичная [CVE-2009-1537] - Критичная [CVE-2009-1538] - Критичная [CVE-2009-1539] - Критичная [CVE-2009-1545] - Критичная [CVE-2009-1546] - Высокая [CVE-2009-1761] - Средняя [CVE-2009-1808] - Средняя [CVE-2009-1920] - Критичная [CVE-2009-1922] - Средняя [CVE-2009-1923] - Критичная [CVE-2009-1924] - Критичная [CVE-2009-1925] - Критичная [CVE-2009-1926] - Высокая [CVE-2009-1928] - Высокая [CVE-2009-1929] - Критичная [CVE-2009-1930] - Критичная [CVE-2009-2357] - Критичная [CVE-2009-2484] - Критичная [CVE-2009-2494] - Критичная [CVE-2009-2498] - Критичная [CVE-2009-2499] - Высокая [CVE-2009-2500] - Критичная [CVE-2009-2501] - Критичная [CVE-2009-2502] - Критичная [CVE-2009-2503] - Критичная [CVE-2009-2504] - Критичная [CVE-2009-2505] - Критичная [CVE-2009-2507] - Критичная [CVE-2009-2508] - Средняя [CVE-2009-2509] - Критичная [CVE-2009-2510] - Средняя [CVE-2009-2511] - Высокая [CVE-2009-2513] - Высокая [CVE-2009-2514] - Критичная [CVE-2009-2515] - Высокая [CVE-2009-2516] - Средняя [CVE-2009-2517] - Средняя [CVE-2009-2519] - Критичная [CVE-2009-2524] - Высокая [CVE-2009-2525] - Критичная [CVE-2009-2526] - Высокая [CVE-2009-2527] - Критичная [CVE-2009-2532] - Критичная [CVE-2009-2544] - Средняя [CVE-2009-2653] - Средняя [CVE-2009-2655] - Средняя [CVE-2009-2764] - Средняя [CVE-2009-3019] - Средняя [CVE-2009-3020] - Высокая [CVE-2009-3103] - Критичная [CVE-2009-3126] - Критичная [CVE-2009-3294] - Средняя [CVE-2009-3675] - Средняя [CVE-2009-3676] - Высокая [CVE-2009-3677] - Критичная [CVE-2009-3678] - Критичная [CVE-2009-4210] - Критичная [CVE-2009-4309] - Критичная [CVE-2009-4310] - Критичная [CVE-2009-4311] - Критичная [CVE-2009-4312] - Критичная [CVE-2009-4313] - Критичная [CVE-2010-0016] - Критичная [CVE-2010-0017] - Критичная [CVE-2010-0018] - Критичная [CVE-2010-0019] - Критичная [CVE-2010-0020] - Критичная [CVE-2010-0021] - Высокая [CVE-2010-0022] - Высокая [CVE-2010-0023] - Средняя [CVE-2010-0024] - Средняя [CVE-2010-0025] - Средняя [CVE-2010-0026] - Средняя [CVE-2010-0027] - Критичная [CVE-2010-0028] - Критичная [CVE-2010-0035] - Средняя [CVE-2010-0231] - Критичная [CVE-2010-0232] - Высокая [CVE-2010-0233] - Высокая [CVE-2010-0234] - Средняя [CVE-2010-0235] - Средняя [CVE-2010-0236] - Высокая [CVE-2010-0237] - Средняя [CVE-2010-0238] - Средняя [CVE-2010-0239] - Критичная [CVE-2010-0240] - Критичная [CVE-2010-0241] - Критичная [CVE-2010-0242] - Высокая [CVE-2010-0249] - Критичная [CVE-2010-0250] - Критичная [CVE-2010-0252] - Критичная [CVE-2010-0265] - Критичная [CVE-2010-0268] - Критичная [CVE-2010-0269] - Критичная [CVE-2010-0270] - Критичная [CVE-2010-0278] - Средняя [CVE-2010-0378] - Критичная [CVE-2010-0379] - Критичная [CVE-2010-0476] - Критичная [CVE-2010-0477] - Критичная [CVE-2010-0478] - Критичная [CVE-2010-0480] - Критичная [CVE-2010-0481] - Средняя [CVE-2010-0482] - Средняя [CVE-2010-0483] - Высокая [CVE-2010-0484] - Средняя [CVE-2010-0485] - Средняя [CVE-2010-0486] - Критичная [CVE-2010-0487] - Критичная [CVE-2010-0718] - Средняя [CVE-2010-0719] - Средняя [CVE-2010-0805] - Критичная [CVE-2010-0808] - Низкая [CVE-2010-0810] - Средняя [CVE-2010-0811] - Критичная [CVE-2010-0812] - Средняя [CVE-2010-0818] - Критичная [CVE-2010-0819] - Высокая [CVE-2010-0820] - Критичная [CVE-2010-0917] - Высокая [CVE-2010-1042] - Средняя [CVE-2010-1098] - Высокая [CVE-2010-1117] - Высокая [CVE-2010-1118] - Критичная [CVE-2010-1175] - Критичная [CVE-2010-1225] - Критичная [CVE-2010-1255] - Средняя [CVE-2010-1263] - Критичная [CVE-2010-1264] - Средняя [CVE-2010-1689] - Средняя [CVE-2010-1690] - Средняя [CVE-2010-1734] - Средняя [CVE-2010-1735] - Средняя [CVE-2010-1880] - Критичная [CVE-2010-1882] - Критичная [CVE-2010-1883] - Критичная [CVE-2010-1885] - Критичная [CVE-2010-1886] - Средняя [CVE-2010-1887] - Средняя [CVE-2010-1888] - Средняя [CVE-2010-1889] - Высокая [CVE-2010-1890] - Средняя [CVE-2010-1891] - Средняя [CVE-2010-1892] - Высокая [CVE-2010-1893] - Средняя [CVE-2010-1894] - Высокая [CVE-2010-1895] - Высокая [CVE-2010-1896] - Высокая [CVE-2010-1897] - Высокая [CVE-2010-1898] - Критичная [CVE-2010-2091] - Средняя [CVE-2010-2265] - Средняя [CVE-2010-2549] - Высокая [CVE-2010-2550] - Критичная [CVE-2010-2551] - Высокая [CVE-2010-2552] - Высокая [CVE-2010-2553] - Критичная [CVE-2010-2554] - Средняя [CVE-2010-2555] - Средняя [CVE-2010-2563] - Критичная [CVE-2010-2564] - Критичная [CVE-2010-2566] - Критичная [CVE-2010-2568] - Критичная [CVE-2010-2731] - Средняя [CVE-2010-2738] - Критичная [CVE-2010-2739] - Высокая [CVE-2010-2740] - Высокая [CVE-2010-2741] - Высокая [CVE-2010-2743] - Высокая [CVE-2010-2744] - Высокая [CVE-2010-2745] - Критичная [CVE-2010-2746] - Высокая [CVE-2010-3138] - Критичная [CVE-2010-3140] - Критичная [CVE-2010-3143] - Критичная [CVE-2010-3144] - Критичная [CVE-2010-3145] - Критичная [CVE-2010-3147] - Критичная [CVE-2010-3223] - Высокая [CVE-2010-3225] - Высокая [CVE-2010-3227] - Критичная [CVE-2010-3229] - Высокая [CVE-2010-3243] - Средняя [CVE-2010-3324] - Средняя [CVE-2010-3338] - Высокая [CVE-2010-3888] - Высокая [CVE-2010-3889] - Высокая [CVE-2010-3937] - Средняя [CVE-2010-3939] - Высокая [CVE-2010-3940] - Высокая [CVE-2010-3941] - Высокая [CVE-2010-3942] - Высокая [CVE-2010-3943] - Высокая [CVE-2010-3944] - Высокая [CVE-2010-3956] - Критичная [CVE-2010-3957] - Средняя [CVE-2010-3959] - Средняя [CVE-2010-3960] - Средняя [CVE-2010-3961] - Высокая [CVE-2010-3963] - Высокая [CVE-2010-3965] - Критичная [CVE-2010-3966] - Критичная [CVE-2010-3967] - Критичная [CVE-2010-3970] - Критичная [CVE-2010-3973] - Критичная [CVE-2010-3974] - Высокая [CVE-2010-4182] - Критичная [CVE-2010-4398] - Высокая [CVE-2010-4562] - Средняя [CVE-2010-4669] - Высокая [CVE-2010-4701] - Высокая [CVE-2010-5082] - Критичная [CVE-2011-0026] - Критичная [CVE-2011-0027] - Критичная [CVE-2011-0028] - Критичная [CVE-2011-0030] - Средняя [CVE-2011-0031] - Средняя [CVE-2011-0032] - Критичная [CVE-2011-0033] - Критичная [CVE-2011-0034] - Критичная [CVE-2011-0037] - Высокая [CVE-2011-0039] - Высокая [CVE-2011-0040] - Средняя [CVE-2011-0041] - Критичная [CVE-2011-0042] - Критичная [CVE-2011-0043] - Высокая [CVE-2011-0045] - Высокая [CVE-2011-0086] - Высокая [CVE-2011-0087] - Высокая [CVE-2011-0088] - Высокая [CVE-2011-0089] - Высокая [CVE-2011-0090] - Высокая [CVE-2011-0091] - Средняя [CVE-2011-0096] - Средняя [CVE-2011-0347] - Критичная [CVE-2011-0627] - Критичная [CVE-2011-0638] - Средняя [CVE-2011-0654] - Критичная [CVE-2011-0657] - Высокая [CVE-2011-0658] - Критичная [CVE-2011-0660] - Критичная [CVE-2011-0661] - Критичная [CVE-2011-0662] - Высокая [CVE-2011-0665] - Высокая [CVE-2011-0666] - Высокая [CVE-2011-0667] - Высокая [CVE-2011-0670] - Высокая [CVE-2011-0671] - Высокая [CVE-2011-0672] - Высокая [CVE-2011-0673] - Высокая [CVE-2011-0674] - Высокая [CVE-2011-0675] - Высокая [CVE-2011-0676] - Высокая [CVE-2011-0677] - Высокая [CVE-2011-1068] - Низкая [CVE-2011-1225] - Высокая [CVE-2011-1226] - Высокая [CVE-2011-1227] - Высокая [CVE-2011-1228] - Высокая [CVE-2011-1229] - Высокая [CVE-2011-1230] - Высокая [CVE-2011-1231] - Высокая [CVE-2011-1232] - Высокая [CVE-2011-1233] - Высокая [CVE-2011-1234] - Высокая [CVE-2011-1235] - Высокая [CVE-2011-1236] - Высокая [CVE-2011-1237] - Высокая [CVE-2011-1238] - Высокая [CVE-2011-1239] - Высокая [CVE-2011-1240] - Высокая [CVE-2011-1241] - Высокая [CVE-2011-1242] - Высокая [CVE-2011-1243] - Критичная [CVE-2011-1247] - Критичная [CVE-2011-1248] - Критичная [CVE-2011-1249] - Высокая [CVE-2011-1252] - Средняя [CVE-2011-1263] - Средняя [CVE-2011-1264] - Средняя [CVE-2011-1265] - Высокая [CVE-2011-1267] - Высокая [CVE-2011-1268] - Критичная [CVE-2011-1281] - Высокая [CVE-2011-1282] - Высокая [CVE-2011-1283] - Высокая [CVE-2011-1284] - Высокая [CVE-2011-1346] - Критичная [CVE-2011-1347] - Высокая [CVE-2011-1652] - Средняя [CVE-2011-1713] - Средняя [CVE-2011-1868] - Критичная [CVE-2011-1869] - Высокая [CVE-2011-1870] - Высокая [CVE-2011-1871] - Высокая [CVE-2011-1872] - Средняя [CVE-2011-1873] - Критичная [CVE-2011-1874] - Высокая [CVE-2011-1875] - Высокая [CVE-2011-1876] - Высокая [CVE-2011-1877] - Высокая [CVE-2011-1878] - Высокая [CVE-2011-1879] - Высокая [CVE-2011-1880] - Высокая [CVE-2011-1881] - Высокая [CVE-2011-1882] - Высокая [CVE-2011-1883] - Высокая [CVE-2011-1884] - Высокая [CVE-2011-1885] - Высокая [CVE-2011-1886] - Низкая [CVE-2011-1887] - Высокая [CVE-2011-1888] - Высокая [CVE-2011-1891] - Средняя [CVE-2011-1892] - Средняя [CVE-2011-1893] - Средняя [CVE-2011-1894] - Средняя [CVE-2011-1965] - Высокая [CVE-2011-1966] - Критичная [CVE-2011-1967] - Высокая [CVE-2011-1968] - Высокая [CVE-2011-1970] - Средняя [CVE-2011-1971] - Средняя [CVE-2011-1974] - Высокая [CVE-2011-1975] - Критичная [CVE-2011-1984] - Высокая [CVE-2011-1985] - Высокая [CVE-2011-1991] - Критичная [CVE-2011-2002] - Средняя [CVE-2011-2003] - Критичная [CVE-2011-2004] - Высокая [CVE-2011-2005] - Высокая [CVE-2011-2009] - Критичная [CVE-2011-2011] - Высокая [CVE-2011-2013] - Критичная [CVE-2011-2014] - Критичная [CVE-2011-2016] - Критичная [CVE-2011-2018] - Высокая [CVE-2011-2019] - Критичная [CVE-2011-3389] - Средняя [CVE-2011-3397] - Критичная [CVE-2011-3400] - Критичная [CVE-2011-3401] - Критичная [CVE-2011-3402] - Критичная [CVE-2011-3406] - Критичная [CVE-2011-3408] - Высокая [CVE-2011-4434] - Низкая [CVE-2011-4695] - Средняя [CVE-2011-5046] - Критичная [CVE-2011-5279] - Средняя [CVE-2012-0001] - Критичная [CVE-2012-0002] - Критичная [CVE-2012-0003] - Критичная [CVE-2012-0004] - Критичная [CVE-2012-0005] - Средняя [CVE-2012-0006] - Средняя [CVE-2012-0009] - Критичная [CVE-2012-0013] - Критичная [CVE-2012-0148] - Высокая [CVE-2012-0149] - Высокая [CVE-2012-0150] - Критичная [CVE-2012-0151] - Критичная [CVE-2012-0152] - Средняя [CVE-2012-0154] - Высокая [CVE-2012-0156] - Средняя [CVE-2012-0157] - Высокая [CVE-2012-0159] - Критичная [CVE-2012-0164] - Средняя [CVE-2012-0165] - Критичная [CVE-2012-0173] - Критичная [CVE-2012-0174] - Низкая [CVE-2012-0175] - Критичная [CVE-2012-0176] - Критичная [CVE-2012-0178] - Высокая [CVE-2012-0179] - Высокая [CVE-2012-0180] - Высокая [CVE-2012-0181] - Высокая [CVE-2012-1194] - Средняя [CVE-2012-1527] - Критичная [CVE-2012-1528] - Критичная [CVE-2012-1537] - Критичная [CVE-2012-1848] - Высокая [CVE-2012-1850] - Средняя [CVE-2012-1851] - Критичная [CVE-2012-1852] - Критичная [CVE-2012-1853] - Критичная [CVE-2012-1863] - Средняя [CVE-2012-1864] - Высокая [CVE-2012-1865] - Высокая [CVE-2012-1866] - Высокая [CVE-2012-1867] - Высокая [CVE-2012-1868] - Средняя [CVE-2012-1870] - Средняя [CVE-2012-1890] - Высокая [CVE-2012-1891] - Критичная [CVE-2012-1893] - Высокая [CVE-2012-1945] - Низкая [CVE-2012-2520] - Средняя [CVE-2012-2526] - Критичная [CVE-2012-2527] - Высокая [CVE-2012-2529] - Высокая [CVE-2012-2530] - Высокая [CVE-2012-2551] - Средняя [CVE-2012-2553] - Высокая [CVE-2012-2556] - Критичная [CVE-2012-2897] - Критичная [CVE-2012-2971] - Высокая [CVE-2012-2972] - Средняя [CVE-2012-2993] - Низкая [CVE-2012-4774] - Критичная [CVE-2012-4786] - Критичная [CVE-2012-5362] - Высокая [CVE-2012-5364] - Высокая [CVE-2013-0001] - Средняя [CVE-2013-0002] - Критичная [CVE-2013-0005] - Высокая [CVE-2013-0008] - Высокая [CVE-2013-0011] - Критичная [CVE-2013-0013] - Средняя [CVE-2013-0073] - Критичная [CVE-2013-0075] - Высокая [CVE-2013-0076] - Высокая [CVE-2013-0077] - Критичная [CVE-2013-0078] - Высокая [CVE-2013-0096] - Средняя [CVE-2013-0810] - Критичная [CVE-2013-0941] - Низкая [CVE-2013-1248] - Средняя [CVE-2013-1249] - Средняя [CVE-2013-1250] - Средняя [CVE-2013-1251] - Средняя [CVE-2013-1252] - Средняя [CVE-2013-1253] - Средняя [CVE-2013-1254] - Средняя [CVE-2013-1255] - Средняя [CVE-2013-1256] - Средняя [CVE-2013-1257] - Средняя [CVE-2013-1258] - Средняя [CVE-2013-1259] - Средняя [CVE-2013-1260] - Средняя [CVE-2013-1261] - Средняя [CVE-2013-1262] - Средняя [CVE-2013-1263] - Средняя [CVE-2013-1264] - Средняя [CVE-2013-1265] - Средняя [CVE-2013-1266] - Средняя [CVE-2013-1267] - Средняя [CVE-2013-1268] - Средняя [CVE-2013-1269] - Средняя [CVE-2013-1270] - Средняя [CVE-2013-1271] - Средняя [CVE-2013-1272] - Средняя [CVE-2013-1273] - Средняя [CVE-2013-1274] - Средняя [CVE-2013-1275] - Средняя [CVE-2013-1276] - Средняя [CVE-2013-1277] - Средняя [CVE-2013-1278] - Высокая [CVE-2013-1279] - Высокая [CVE-2013-1280] - Высокая [CVE-2013-1281] - Высокая [CVE-2013-1283] - Средняя [CVE-2013-1284] - Средняя [CVE-2013-1285] - Высокая [CVE-2013-1286] - Высокая [CVE-2013-1287] - Высокая [CVE-2013-1291] - Высокая [CVE-2013-1292] - Средняя [CVE-2013-1293] - Средняя [CVE-2013-1294] - Средняя [CVE-2013-1295] - Высокая [CVE-2013-1299] - Средняя [CVE-2013-1300] - Высокая [CVE-2013-1305] - Высокая [CVE-2013-1313] - Критичная [CVE-2013-1332] - Высокая [CVE-2013-1333] - Высокая [CVE-2013-1334] - Высокая [CVE-2013-1337] - Высокая [CVE-2013-1339] - Критичная [CVE-2013-1340] - Высокая [CVE-2013-1341] - Высокая [CVE-2013-1342] - Высокая [CVE-2013-1343] - Высокая [CVE-2013-1344] - Высокая [CVE-2013-1345] - Высокая [CVE-2013-2552] - Высокая [CVE-2013-2553] - Высокая [CVE-2013-2554] - Высокая [CVE-2013-2556] - Высокая [CVE-2013-2558] - Критичная [CVE-2013-3127] - Критичная [CVE-2013-3128] - Критичная [CVE-2013-3136] - Средняя [CVE-2013-3138] - Высокая [CVE-2013-3154] - Средняя [CVE-2013-3167] - Высокая [CVE-2013-3172] - Средняя [CVE-2013-3173] - Высокая [CVE-2013-3174] - Критичная [CVE-2013-3181] - Критичная [CVE-2013-3182] - Высокая [CVE-2013-3183] - Высокая [CVE-2013-3185] - Средняя [CVE-2013-3186] - Высокая [CVE-2013-3195] - Критичная [CVE-2013-3196] - Высокая [CVE-2013-3197] - Высокая [CVE-2013-3198] - Высокая [CVE-2013-3200] - Высокая [CVE-2013-3660] - Средняя [CVE-2013-3661] - Средняя [CVE-2013-3862] - Средняя [CVE-2013-3863] - Критичная [CVE-2013-3864] - Высокая [CVE-2013-3865] - Высокая [CVE-2013-3866] - Высокая [CVE-2013-3868] - Средняя [CVE-2013-3869] - Средняя [CVE-2013-3876] - Высокая [CVE-2013-3879] - Высокая [CVE-2013-3880] - Низкая [CVE-2013-3881] - Высокая [CVE-2013-3887] - Средняя [CVE-2013-3888] - Высокая [CVE-2013-3894] - Критичная [CVE-2013-3898] - Высокая [CVE-2013-3899] - Высокая [CVE-2013-3900] - Высокая [CVE-2013-3902] - Высокая [CVE-2013-3903] - Средняя [CVE-2013-3906] - Критичная [CVE-2013-3907] - Высокая [CVE-2013-3918] - Критичная [CVE-2013-3940] - Критичная [CVE-2013-4858] - Средняя [CVE-2013-5056] - Критичная [CVE-2013-5058] - Средняя [CVE-2013-5065] - Высокая [CVE-2013-6230] - Средняя [CVE-2013-6801] - Высокая [CVE-2013-6999] - Средняя [CVE-2013-7331] - Средняя [CVE-2013-7332] - Средняя [CVE-2013-7369] - Высокая [CVE-2014-0251] - Критичная [CVE-2014-0254] - Высокая [CVE-2014-0255] - Средняя [CVE-2014-0256] - Средняя [CVE-2014-0262] - Высокая [CVE-2014-0263] - Критичная [CVE-2014-0266] - Высокая [CVE-2014-0296] - Средняя [CVE-2014-0300] - Высокая [CVE-2014-0301] - Критичная [CVE-2014-0315] - Средняя [CVE-2014-0317] - Средняя [CVE-2014-0318] - Высокая [CVE-2014-0323] - Средняя [CVE-2014-1767] - Высокая [CVE-2014-1807] - Высокая [CVE-2014-1811] - Средняя [CVE-2014-1812] - Критичная [CVE-2014-1814] - Высокая [CVE-2014-1817] - Критичная [CVE-2014-1818] - Критичная [CVE-2014-1819] - Высокая [CVE-2014-1824] - Критичная [CVE-2014-2671] - Средняя [CVE-2014-2780] - Средняя [CVE-2014-2781] - Высокая [CVE-2014-2814] - Средняя [CVE-2014-4060] - Средняя [CVE-2014-4064] - Средняя [CVE-2014-4074] - Высокая [CVE-2014-4076] - Высокая [CVE-2014-4077] - Критичная [CVE-2014-4113] - Высокая [CVE-2014-4114] - Критичная [CVE-2014-4115] - Высокая [CVE-2014-4118] - Критичная [CVE-2014-4148] - Критичная [CVE-2014-4971] - Высокая [CVE-2014-6317] - Высокая [CVE-2014-6318] - Средняя [CVE-2014-6321] - Критичная [CVE-2014-6322] - Средняя [CVE-2014-6324] - Критичная [CVE-2014-6332] - Критичная [CVE-2014-6352] - Критичная [CVE-2014-6355] - Средняя [CVE-2015-0001] - Низкая [CVE-2015-0002] - Высокая [CVE-2015-0003] - Средняя [CVE-2015-0004] - Высокая [CVE-2015-0005] - Средняя [CVE-2015-0006] - Средняя [CVE-2015-0008] - Высокая [CVE-2015-0009] - Низкая [CVE-2015-0010] - Низкая [CVE-2015-0011] - Средняя [CVE-2015-0014] - Критичная [CVE-2015-0015] - Высокая [CVE-2015-0016] - Критичная [CVE-2015-0057] - Высокая [CVE-2015-0058] - Высокая [CVE-2015-0059] - Средняя [CVE-2015-0060] - Средняя [CVE-2015-0061] - Средняя [CVE-2015-0062] - Высокая [CVE-2015-0073] - Высокая [CVE-2015-0074] - Средняя [CVE-2015-0075] - Высокая [CVE-2015-0076] - Средняя [CVE-2015-0077] - Низкая [CVE-2015-0078] - Высокая [CVE-2015-0079] - Высокая [CVE-2015-0080] - Средняя [CVE-2015-0081] - Критичная [CVE-2015-0084] - Низкая [CVE-2015-0085] - Критичная [CVE-2015-0087] - Средняя [CVE-2015-0088] - Критичная [CVE-2015-0089] - Средняя [CVE-2015-0090] - Критичная [CVE-2015-0091] - Критичная [CVE-2015-0092] - Критичная [CVE-2015-0093] - Критичная [CVE-2015-0094] - Низкая [CVE-2015-0095] - Средняя [CVE-2015-0096] - Критичная [CVE-2015-0098] - Высокая [CVE-2015-1635] - Критичная [CVE-2015-1637] - Средняя [CVE-2015-1638] - Средняя [CVE-2015-1643] - Высокая [CVE-2015-1644] - Высокая [CVE-2015-1645] - Критичная [CVE-2015-1647] - Низкая [CVE-2015-1670] - Средняя [CVE-2015-1671] - Критичная [CVE-2015-1673] - Критичная [CVE-2015-1674] - Средняя [CVE-2015-1675] - Критичная [CVE-2015-1676] - Низкая [CVE-2015-1677] - Низкая [CVE-2015-1678] - Низкая [CVE-2015-1679] - Низкая [CVE-2015-1680] - Низкая [CVE-2015-1681] - Низкая [CVE-2015-1695] - Критичная [CVE-2015-1696] - Критичная [CVE-2015-1697] - Критичная [CVE-2015-1698] - Критичная [CVE-2015-1699] - Критичная [CVE-2015-1701] - Высокая [CVE-2015-1702] - Средняя [CVE-2015-1716] - Средняя [CVE-2015-1719] - Низкая [CVE-2015-1720] - Высокая [CVE-2015-1721] - Высокая [CVE-2015-1722] - Высокая [CVE-2015-1723] - Высокая [CVE-2015-1724] - Высокая [CVE-2015-1725] - Высокая [CVE-2015-1726] - Высокая [CVE-2015-1727] - Высокая [CVE-2015-1728] - Критичная [CVE-2015-1756] - Критичная [CVE-2015-1757] - Средняя [CVE-2015-1758] - Средняя [CVE-2015-1768] - Высокая [CVE-2015-1769] - Высокая [CVE-2015-2360] - Высокая [CVE-2015-2361] - Высокая [CVE-2015-2362] - Высокая [CVE-2015-2363] - Высокая [CVE-2015-2364] - Высокая [CVE-2015-2365] - Высокая [CVE-2015-2366] - Высокая [CVE-2015-2367] - Низкая [CVE-2015-2368] - Средняя [CVE-2015-2369] - Средняя [CVE-2015-2371] - Средняя [CVE-2015-2373] - Критичная [CVE-2015-2374] - Низкая [CVE-2015-2381] - Низкая [CVE-2015-2382] - Низкая [CVE-2015-2387] - Высокая [CVE-2015-2416] - Средняя [CVE-2015-2417] - Средняя [CVE-2015-2423] - Средняя [CVE-2015-2426] - Критичная [CVE-2015-2428] - Низкая [CVE-2015-2429] - Критичная [CVE-2015-2430] - Критичная [CVE-2015-2432] - Критичная [CVE-2015-2433] - Низкая [CVE-2015-2435] - Критичная [CVE-2015-2453] - Средняя [CVE-2015-2454] - Низкая [CVE-2015-2455] - Критичная [CVE-2015-2456] - Критичная [CVE-2015-2458] - Критичная [CVE-2015-2459] - Критичная [CVE-2015-2460] - Критичная [CVE-2015-2461] - Критичная [CVE-2015-2462] - Критичная [CVE-2015-2463] - Критичная [CVE-2015-2464] - Критичная [CVE-2015-2465] - Низкая [CVE-2015-2472] - Средняя [CVE-2015-2473] - Критичная [CVE-2015-2474] - Критичная [CVE-2015-2475] - Средняя [CVE-2015-2476] - Низкая [CVE-2015-2478] - Высокая [CVE-2015-2506] - Критичная [CVE-2015-2507] - Высокая [CVE-2015-2508] - Высокая [CVE-2015-2509] - Критичная [CVE-2015-2510] - Критичная [CVE-2015-2511] - Средняя [CVE-2015-2512] - Высокая [CVE-2015-2513] - Критичная [CVE-2015-2514] - Критичная [CVE-2015-2515] - Критичная [CVE-2015-2516] - Средняя [CVE-2015-2517] - Средняя [CVE-2015-2518] - Средняя [CVE-2015-2519] - Критичная [CVE-2015-2524] - Высокая [CVE-2015-2525] - Высокая [CVE-2015-2527] - Высокая [CVE-2015-2528] - Высокая [CVE-2015-2529] - Низкая [CVE-2015-2530] - Критичная [CVE-2015-2534] - Низкая [CVE-2015-2535] - Средняя [CVE-2015-2546] - Средняя [CVE-2015-2548] - Критичная [CVE-2015-2549] - Высокая [CVE-2015-2550] - Высокая [CVE-2015-2552] - Высокая [CVE-2015-2553] - Высокая [CVE-2015-2554] - Высокая [CVE-2015-4949] - Низкая [CVE-2015-6095] - Средняя [CVE-2015-6097] - Критичная [CVE-2015-6098] - Высокая [CVE-2015-6100] - Средняя [CVE-2015-6101] - Средняя [CVE-2015-6102] - Низкая [CVE-2015-6103] - Критичная [CVE-2015-6104] - Критичная [CVE-2015-6106] - Критичная [CVE-2015-6107] - Критичная [CVE-2015-6108] - Критичная [CVE-2015-6109] - Низкая [CVE-2015-6111] - Средняя [CVE-2015-6112] - Средняя [CVE-2015-6113] - Низкая [CVE-2015-6125] - Критичная [CVE-2015-6126] - Высокая [CVE-2015-6127] - Средняя [CVE-2015-6128] - Высокая [CVE-2015-6130] - Критичная [CVE-2015-6131] - Критичная [CVE-2015-6132] - Высокая [CVE-2015-6133] - Высокая [CVE-2015-6171] - Высокая [CVE-2015-6173] - Высокая [CVE-2015-6174] - Высокая [CVE-2015-6175] - Высокая [CVE-2016-0006] - Высокая [CVE-2016-0007] - Высокая [CVE-2016-0008] - Средняя [CVE-2016-0009] - Высокая [CVE-2016-0014] - Высокая [CVE-2016-0015] - Высокая [CVE-2016-0016] - Высокая [CVE-2016-0018] - Высокая [CVE-2016-0019] - Высокая [CVE-2016-0020] - Высокая [CVE-2016-0026] - Высокая [CVE-2016-0036] - Высокая [CVE-2016-0037] - Высокая [CVE-2016-0038] - Высокая [CVE-2016-0040] - Высокая [CVE-2016-0041] - Высокая [CVE-2016-0042] - Высокая [CVE-2016-0044] - Высокая [CVE-2016-0046] - Высокая [CVE-2016-0047] - Высокая [CVE-2016-0048] - Высокая [CVE-2016-0049] - Средняя [CVE-2016-0050] - Средняя [CVE-2016-0051] - Высокая [CVE-2016-0058] - Высокая [CVE-2016-0070] - Средняя [CVE-2016-0073] - Средняя [CVE-2016-0075] - Средняя [CVE-2016-0079] - Средняя [CVE-2016-0087] - Высокая [CVE-2016-0088] - Критичная [CVE-2016-0089] - Высокая [CVE-2016-0090] - Высокая [CVE-2016-0091] - Высокая [CVE-2016-0092] - Высокая [CVE-2016-0093] - Высокая [CVE-2016-0094] - Высокая [CVE-2016-0095] - Высокая [CVE-2016-0096] - Высокая [CVE-2016-0098] - Высокая [CVE-2016-0099] - Высокая [CVE-2016-0100] - Высокая [CVE-2016-0101] - Высокая [CVE-2016-0117] - Высокая [CVE-2016-0118] - Высокая [CVE-2016-0120] - Средняя [CVE-2016-0121] - Высокая [CVE-2016-0133] - Средняя [CVE-2016-0135] - Высокая [CVE-2016-0142] - Высокая [CVE-2016-0143] - Высокая [CVE-2016-0145] - Высокая [CVE-2016-0150] - Высокая [CVE-2016-0151] - Высокая [CVE-2016-0152] - Высокая [CVE-2016-0153] - Высокая [CVE-2016-0165] - Высокая [CVE-2016-0167] - Высокая [CVE-2016-0168] - Средняя [CVE-2016-0169] - Средняя [CVE-2016-0170] - Высокая [CVE-2016-0171] - Высокая [CVE-2016-0173] - Высокая [CVE-2016-0174] - Высокая [CVE-2016-0175] - Низкая [CVE-2016-0176] - Высокая [CVE-2016-0179] - Высокая [CVE-2016-0180] - Высокая [CVE-2016-0181] - Средняя [CVE-2016-0182] - Высокая [CVE-2016-0183] - Высокая [CVE-2016-0184] - Высокая [CVE-2016-0185] - Высокая [CVE-2016-0190] - Средняя [CVE-2016-0195] - Высокая [CVE-2016-0196] - Высокая [CVE-2016-0197] - Высокая [CVE-2016-3201] - Средняя [CVE-2016-3203] - Высокая [CVE-2016-3209] - Средняя [CVE-2016-3213] - Высокая [CVE-2016-3215] - Средняя [CVE-2016-3216] - Средняя [CVE-2016-3218] - Высокая [CVE-2016-3219] - Высокая [CVE-2016-3220] - Высокая [CVE-2016-3221] - Высокая [CVE-2016-3223] - Высокая [CVE-2016-3225] - Высокая [CVE-2016-3226] - Средняя [CVE-2016-3227] - Критичная [CVE-2016-3228] - Высокая [CVE-2016-3230] - Средняя [CVE-2016-3232] - Средняя [CVE-2016-3236] - Критичная [CVE-2016-3237] - Высокая [CVE-2016-3238] - Высокая [CVE-2016-3239] - Высокая [CVE-2016-3249] - Высокая [CVE-2016-3250] - Высокая [CVE-2016-3251] - Низкая [CVE-2016-3252] - Высокая [CVE-2016-3254] - Высокая [CVE-2016-3256] - Средняя [CVE-2016-3258] - Средняя [CVE-2016-3262] - Средняя [CVE-2016-3263] - Средняя [CVE-2016-3266] - Высокая [CVE-2016-3270] - Высокая [CVE-2016-3272] - Низкая [CVE-2016-3286] - Высокая [CVE-2016-3287] - Средняя [CVE-2016-3298] - Средняя [CVE-2016-3299] - Средняя [CVE-2016-3300] - Высокая [CVE-2016-3301] - Высокая [CVE-2016-3302] - Средняя [CVE-2016-3303] - Высокая [CVE-2016-3304] - Высокая [CVE-2016-3305] - Высокая [CVE-2016-3306] - Высокая [CVE-2016-3308] - Высокая [CVE-2016-3309] - Высокая [CVE-2016-3310] - Высокая [CVE-2016-3311] - Высокая [CVE-2016-3312] - Критичная [CVE-2016-3319] - Высокая [CVE-2016-3320] - Средняя [CVE-2016-3332] - Высокая [CVE-2016-3333] - Высокая [CVE-2016-3334] - Высокая [CVE-2016-3335] - Высокая [CVE-2016-3338] - Высокая [CVE-2016-3340] - Высокая [CVE-2016-3341] - Высокая [CVE-2016-3342] - Высокая [CVE-2016-3343] - Высокая [CVE-2016-3344] - Низкая [CVE-2016-3345] - Высокая [CVE-2016-3346] - Высокая [CVE-2016-3348] - Высокая [CVE-2016-3349] - Высокая [CVE-2016-3352] - Высокая [CVE-2016-3354] - Низкая [CVE-2016-3355] - Высокая [CVE-2016-3356] - Высокая [CVE-2016-3368] - Высокая [CVE-2016-3369] - Высокая [CVE-2016-3370] - Средняя [CVE-2016-3371] - Средняя [CVE-2016-3372] - Средняя [CVE-2016-3373] - Средняя [CVE-2016-3374] - Средняя [CVE-2016-3375] - Высокая [CVE-2016-3376] - Высокая [CVE-2016-3393] - Высокая [CVE-2016-3396] - Высокая [CVE-2016-5063] - Средняя [CVE-2016-6848] - Средняя [CVE-2016-7165] - Средняя [CVE-2016-7182] - Критичная [CVE-2016-7184] - Высокая [CVE-2016-7185] - Высокая [CVE-2016-7188] - Высокая [CVE-2016-7205] - Высокая [CVE-2016-7210] - Средняя [CVE-2016-7211] - Высокая [CVE-2016-7212] - Высокая [CVE-2016-7214] - Низкая [CVE-2016-7215] - Высокая [CVE-2016-7216] - Средняя [CVE-2016-7217] - Высокая [CVE-2016-7218] - Средняя [CVE-2016-7219] - Средняя [CVE-2016-7220] - Низкая [CVE-2016-7221] - Высокая [CVE-2016-7222] - Высокая [CVE-2016-7223] - Средняя [CVE-2016-7224] - Средняя [CVE-2016-7237] - Средняя [CVE-2016-7238] - Высокая [CVE-2016-7246] - Высокая [CVE-2016-7247] - Высокая [CVE-2016-7248] - Высокая [CVE-2016-7255] - Высокая [CVE-2016-7256] - Высокая [CVE-2016-7257] - Средняя [CVE-2016-7258] - Средняя [CVE-2016-7259] - Высокая [CVE-2016-7260] - Высокая [CVE-2016-7271] - Высокая [CVE-2016-7272] - Высокая [CVE-2016-7273] - Высокая [CVE-2016-7274] - Высокая [CVE-2016-7278] - Средняя [CVE-2016-7292] - Высокая [CVE-2016-7295] - Средняя [CVE-2016-9192] - Высокая [CVE-2016-9459] - Средняя [CVE-2017-0001] - Высокая [CVE-2017-0004] - Высокая [CVE-2017-0005] - Высокая [CVE-2017-0007] - Средняя [CVE-2017-0014] - Высокая [CVE-2017-0016] - Средняя [CVE-2017-0021] - Критичная [CVE-2017-0022] - Средняя [CVE-2017-0024] - Высокая [CVE-2017-0025] - Высокая [CVE-2017-0026] - Высокая [CVE-2017-0038] - Средняя [CVE-2017-0039] - Высокая [CVE-2017-0042] - Низкая [CVE-2017-0043] - Средняя [CVE-2017-0047] - Высокая [CVE-2017-0050] - Высокая [CVE-2017-0051] - Средняя [CVE-2017-0055] - Средняя [CVE-2017-0056] - Высокая [CVE-2017-0057] - Средняя [CVE-2017-0058] - Средняя [CVE-2017-0060] - Средняя [CVE-2017-0061] - Средняя [CVE-2017-0062] - Средняя [CVE-2017-0066] - Средняя [CVE-2017-0072] - Высокая [CVE-2017-0073] - Средняя [CVE-2017-0074] - Средняя [CVE-2017-0075] - Высокая [CVE-2017-0076] - Средняя [CVE-2017-0078] - Высокая [CVE-2017-0080] - Высокая [CVE-2017-0081] - Высокая [CVE-2017-0082] - Высокая [CVE-2017-0083] - Высокая [CVE-2017-0084] - Высокая [CVE-2017-0085] - Средняя [CVE-2017-0086] - Высокая [CVE-2017-0087] - Высокая [CVE-2017-0088] - Высокая [CVE-2017-0089] - Высокая [CVE-2017-0090] - Высокая [CVE-2017-0091] - Средняя [CVE-2017-0092] - Средняя [CVE-2017-0095] - Высокая [CVE-2017-0096] - Низкая [CVE-2017-0097] - Средняя [CVE-2017-0098] - Средняя [CVE-2017-0099] - Средняя [CVE-2017-0100] - Высокая [CVE-2017-0101] - Высокая [CVE-2017-0102] - Высокая [CVE-2017-0103] - Высокая [CVE-2017-0104] - Высокая [CVE-2017-0108] - Высокая [CVE-2017-0109] - Высокая [CVE-2017-0111] - Средняя [CVE-2017-0112] - Средняя [CVE-2017-0113] - Средняя [CVE-2017-0114] - Средняя [CVE-2017-0115] - Средняя [CVE-2017-0116] - Средняя [CVE-2017-0117] - Средняя [CVE-2017-0118] - Средняя [CVE-2017-0119] - Средняя [CVE-2017-0120] - Средняя [CVE-2017-0121] - Средняя [CVE-2017-0122] - Средняя [CVE-2017-0123] - Средняя [CVE-2017-0124] - Средняя [CVE-2017-0125] - Средняя [CVE-2017-0126] - Средняя [CVE-2017-0127] - Средняя [CVE-2017-0128] - Средняя [CVE-2017-0135] - Средняя [CVE-2017-0140] - Средняя [CVE-2017-0143] - Высокая [CVE-2017-0144] - Высокая [CVE-2017-0145] - Высокая [CVE-2017-0146] - Высокая [CVE-2017-0147] - Средняя [CVE-2017-0148] - Высокая [CVE-2017-0154] - Средняя [CVE-2017-0155] - Высокая [CVE-2017-0156] - Высокая [CVE-2017-0158] - Высокая [CVE-2017-0161] - Высокая [CVE-2017-0165] - Высокая [CVE-2017-0171] - Средняя [CVE-2017-0173] - Средняя [CVE-2017-0176] - Высокая [CVE-2017-0178] - Средняя [CVE-2017-0179] - Средняя [CVE-2017-0182] - Средняя [CVE-2017-0183] - Средняя [CVE-2017-0185] - Средняя [CVE-2017-0186] - Средняя [CVE-2017-0190] - Средняя [CVE-2017-0192] - Средняя [CVE-2017-0193] - Высокая [CVE-2017-0199] - Высокая [CVE-2017-0211] - Средняя [CVE-2017-0212] - Высокая [CVE-2017-0213] - Средняя [CVE-2017-0214] - Высокая [CVE-2017-0215] - Средняя [CVE-2017-0216] - Средняя [CVE-2017-0218] - Средняя [CVE-2017-0219] - Средняя [CVE-2017-0250] - Высокая [CVE-2017-0258] - Средняя [CVE-2017-0259] - Средняя [CVE-2017-0263] - Высокая [CVE-2017-0267] - Средняя [CVE-2017-0268] - Средняя [CVE-2017-0269] - Средняя [CVE-2017-0270] - Средняя [CVE-2017-0271] - Средняя [CVE-2017-0272] - Высокая [CVE-2017-0273] - Средняя [CVE-2017-0274] - Средняя [CVE-2017-0275] - Средняя [CVE-2017-0276] - Средняя [CVE-2017-0277] - Высокая [CVE-2017-0278] - Высокая [CVE-2017-0279] - Высокая [CVE-2017-0280] - Средняя [CVE-2017-0282] - Средняя [CVE-2017-0283] - Высокая [CVE-2017-0284] - Средняя [CVE-2017-0285] - Средняя [CVE-2017-0290] - Высокая [CVE-2017-0293] - Высокая [CVE-2017-0294] - Высокая [CVE-2017-0295] - Средняя [CVE-2017-0296] - Высокая [CVE-2017-0297] - Средняя [CVE-2017-0298] - Высокая [CVE-2017-0299] - Средняя [CVE-2017-0300] - Средняя [CVE-2017-10769] - Высокая [CVE-2017-10772] - Высокая [CVE-2017-11762] - Высокая [CVE-2017-11763] - Высокая [CVE-2017-11764] - Высокая [CVE-2017-11765] - Средняя [CVE-2017-11766] - Высокая [CVE-2017-11769] - Высокая [CVE-2017-11771] - Критичная [CVE-2017-11772] - Высокая [CVE-2017-11779] - Высокая [CVE-2017-11780] - Высокая [CVE-2017-11781] - Высокая [CVE-2017-11782] - Высокая [CVE-2017-11783] - Высокая [CVE-2017-11784] - Средняя [CVE-2017-11785] - Средняя [CVE-2017-11790] - Средняя [CVE-2017-11791] - Низкая [CVE-2017-11792] - Высокая [CVE-2017-11793] - Высокая [CVE-2017-11794] - Средняя [CVE-2017-11796] - Высокая [CVE-2017-11798] - Высокая [CVE-2017-11799] - Высокая [CVE-2017-11800] - Высокая [CVE-2017-11802] - Высокая [CVE-2017-11803] - Средняя [CVE-2017-11804] - Высокая [CVE-2017-11805] - Высокая [CVE-2017-11806] - Высокая [CVE-2017-11807] - Высокая [CVE-2017-11808] - Высокая [CVE-2017-11809] - Высокая [CVE-2017-11810] - Высокая [CVE-2017-11811] - Высокая [CVE-2017-11812] - Высокая [CVE-2017-11813] - Высокая [CVE-2017-11814] - Средняя [CVE-2017-11815] - Средняя [CVE-2017-11816] - Средняя [CVE-2017-11817] - Средняя [CVE-2017-11818] - Средняя [CVE-2017-11819] - Высокая [CVE-2017-11821] - Высокая [CVE-2017-11822] - Высокая [CVE-2017-11823] - Средняя [CVE-2017-11824] - Высокая [CVE-2017-11827] - Высокая [CVE-2017-11829] - Средняя [CVE-2017-11832] - Средняя [CVE-2017-11833] - Низкая [CVE-2017-11834] - Средняя [CVE-2017-11835] - Средняя [CVE-2017-11836] - Высокая [CVE-2017-11837] - Высокая [CVE-2017-11838] - Высокая [CVE-2017-11839] - Высокая [CVE-2017-11840] - Высокая [CVE-2017-11841] - Высокая [CVE-2017-11843] - Высокая [CVE-2017-11844] - Средняя [CVE-2017-11845] - Высокая [CVE-2017-11846] - Высокая [CVE-2017-11848] - Средняя [CVE-2017-11850] - Низкая [CVE-2017-11852] - Средняя [CVE-2017-11855] - Высокая [CVE-2017-11856] - Высокая [CVE-2017-11858] - Высокая [CVE-2017-11861] - Высокая [CVE-2017-11862] - Высокая [CVE-2017-11863] - Средняя [CVE-2017-11866] - Высокая [CVE-2017-11869] - Высокая [CVE-2017-11870] - Высокая [CVE-2017-11871] - Высокая [CVE-2017-11872] - Средняя [CVE-2017-11873] - Высокая [CVE-2017-11874] - Низкая [CVE-2017-11886] - Высокая [CVE-2017-11887] - Средняя [CVE-2017-11888] - Высокая [CVE-2017-11889] - Высокая [CVE-2017-11890] - Высокая [CVE-2017-11893] - Высокая [CVE-2017-11894] - Высокая [CVE-2017-11895] - Высокая [CVE-2017-11899] - Критичная [CVE-2017-11901] - Высокая [CVE-2017-11903] - Высокая [CVE-2017-11905] - Высокая [CVE-2017-11906] - Средняя [CVE-2017-11907] - Высокая [CVE-2017-11912] - Высокая [CVE-2017-11913] - Высокая [CVE-2017-11914] - Высокая [CVE-2017-11918] - Высокая [CVE-2017-11919] - Средняя [CVE-2017-11927] - Средняя [CVE-2017-11930] - Высокая [CVE-2017-11937] - Высокая [CVE-2017-11940] - Высокая [CVE-2017-12266] - Средняя [CVE-2017-12312] - Средняя [CVE-2017-12313] - Средняя [CVE-2017-16744] - Высокая [CVE-2017-3222] - Критичная [CVE-2017-3823] - Высокая [CVE-2017-4028] - Средняя [CVE-2017-6638] - Высокая [CVE-2017-6639] - Критичная [CVE-2017-6640] - Критичная [CVE-2017-6753] - Высокая [CVE-2017-7269] - Критичная [CVE-2017-8461] - Высокая [CVE-2017-8462] - Средняя [CVE-2017-8464] - Высокая [CVE-2017-8465] - Высокая [CVE-2017-8467] - Высокая [CVE-2017-8468] - Высокая [CVE-2017-8469] - Средняя [CVE-2017-8470] - Средняя [CVE-2017-8471] - Средняя [CVE-2017-8472] - Средняя [CVE-2017-8473] - Средняя [CVE-2017-8474] - Средняя [CVE-2017-8475] - Средняя [CVE-2017-8476] - Средняя [CVE-2017-8477] - Средняя [CVE-2017-8478] - Средняя [CVE-2017-8479] - Средняя [CVE-2017-8480] - Средняя [CVE-2017-8481] - Средняя [CVE-2017-8482] - Средняя [CVE-2017-8483] - Средняя [CVE-2017-8484] - Средняя [CVE-2017-8485] - Средняя [CVE-2017-8486] - Средняя [CVE-2017-8488] - Средняя [CVE-2017-8489] - Средняя [CVE-2017-8490] - Средняя [CVE-2017-8491] - Средняя [CVE-2017-8492] - Средняя [CVE-2017-8493] - Средняя [CVE-2017-8494] - Высокая [CVE-2017-8495] - Высокая [CVE-2017-8496] - Высокая [CVE-2017-8497] - Высокая [CVE-2017-8498] - Средняя [CVE-2017-8499] - Высокая [CVE-2017-8503] - Высокая [CVE-2017-8504] - Средняя [CVE-2017-8515] - Средняя [CVE-2017-8517] - Высокая [CVE-2017-8519] - Высокая [CVE-2017-8520] - Высокая [CVE-2017-8521] - Высокая [CVE-2017-8522] - Высокая [CVE-2017-8523] - Средняя [CVE-2017-8524] - Высокая [CVE-2017-8528] - Высокая [CVE-2017-8529] - Средняя [CVE-2017-8530] - Средняя [CVE-2017-8531] - Средняя [CVE-2017-8534] - Средняя [CVE-2017-8535] - Средняя [CVE-2017-8536] - Средняя [CVE-2017-8537] - Средняя [CVE-2017-8538] - Высокая [CVE-2017-8539] - Средняя [CVE-2017-8540] - Высокая [CVE-2017-8541] - Высокая [CVE-2017-8542] - Средняя [CVE-2017-8543] - Критичная [CVE-2017-8544] - Средняя [CVE-2017-8547] - Высокая [CVE-2017-8548] - Высокая [CVE-2017-8549] - Высокая [CVE-2017-8552] - Высокая [CVE-2017-8553] - Средняя [CVE-2017-8554] - Средняя [CVE-2017-8555] - Средняя [CVE-2017-8556] - Высокая [CVE-2017-8558] - Высокая [CVE-2017-8561] - Высокая [CVE-2017-8562] - Высокая [CVE-2017-8563] - Высокая [CVE-2017-8564] - Средняя [CVE-2017-8566] - Высокая [CVE-2017-8573] - Высокая [CVE-2017-8574] - Высокая [CVE-2017-8575] - Средняя [CVE-2017-8576] - Высокая [CVE-2017-8577] - Высокая [CVE-2017-8578] - Высокая [CVE-2017-8579] - Высокая [CVE-2017-8580] - Высокая [CVE-2017-8581] - Высокая [CVE-2017-8582] - Средняя [CVE-2017-8588] - Высокая [CVE-2017-8589] - Критичная [CVE-2017-8590] - Высокая [CVE-2017-8592] - Средняя [CVE-2017-8593] - Высокая [CVE-2017-8594] - Высокая [CVE-2017-8595] - Высокая [CVE-2017-8596] - Высокая [CVE-2017-8597] - Средняя [CVE-2017-8598] - Высокая [CVE-2017-8599] - Средняя [CVE-2017-8601] - Высокая [CVE-2017-8602] - Средняя [CVE-2017-8603] - Высокая [CVE-2017-8604] - Высокая [CVE-2017-8605] - Высокая [CVE-2017-8606] - Высокая [CVE-2017-8607] - Высокая [CVE-2017-8608] - Высокая [CVE-2017-8609] - Высокая [CVE-2017-8610] - Высокая [CVE-2017-8611] - Средняя [CVE-2017-8617] - Высокая [CVE-2017-8618] - Высокая [CVE-2017-8619] - Высокая [CVE-2017-8628] - Средняя [CVE-2017-8634] - Высокая [CVE-2017-8635] - Высокая [CVE-2017-8636] - Высокая [CVE-2017-8637] - Средняя [CVE-2017-8638] - Высокая [CVE-2017-8639] - Высокая [CVE-2017-8640] - Высокая [CVE-2017-8641] - Высокая [CVE-2017-8642] - Средняя [CVE-2017-8643] - Средняя [CVE-2017-8644] - Средняя [CVE-2017-8645] - Высокая [CVE-2017-8646] - Высокая [CVE-2017-8647] - Высокая [CVE-2017-8648] - Средняя [CVE-2017-8649] - Высокая [CVE-2017-8650] - Средняя [CVE-2017-8651] - Высокая [CVE-2017-8652] - Средняя [CVE-2017-8653] - Высокая [CVE-2017-8655] - Высокая [CVE-2017-8656] - Высокая [CVE-2017-8657] - Высокая [CVE-2017-8659] - Средняя [CVE-2017-8660] - Высокая [CVE-2017-8661] - Высокая [CVE-2017-8662] - Средняя [CVE-2017-8666] - Средняя [CVE-2017-8668] - Средняя [CVE-2017-8669] - Высокая [CVE-2017-8670] - Высокая [CVE-2017-8671] - Высокая [CVE-2017-8672] - Высокая [CVE-2017-8673] - Средняя [CVE-2017-8674] - Высокая [CVE-2017-8675] - Высокая [CVE-2017-8676] - Низкая [CVE-2017-8677] - Средняя [CVE-2017-8678] - Средняя [CVE-2017-8679] - Средняя [CVE-2017-8680] - Средняя [CVE-2017-8681] - Средняя [CVE-2017-8682] - Высокая [CVE-2017-8683] - Средняя [CVE-2017-8684] - Средняя [CVE-2017-8685] - Средняя [CVE-2017-8687] - Средняя [CVE-2017-8688] - Средняя [CVE-2017-8689] - Высокая [CVE-2017-8692] - Высокая [CVE-2017-8693] - Средняя [CVE-2017-8694] - Высокая [CVE-2017-8695] - Средняя [CVE-2017-8696] - Высокая [CVE-2017-8699] - Высокая [CVE-2017-8702] - Высокая [CVE-2017-8703] - Средняя [CVE-2017-8704] - Средняя [CVE-2017-8706] - Средняя [CVE-2017-8707] - Средняя [CVE-2017-8708] - Средняя [CVE-2017-8709] - Средняя [CVE-2017-8710] - Средняя [CVE-2017-8711] - Средняя [CVE-2017-8712] - Средняя [CVE-2017-8713] - Средняя [CVE-2017-8714] - Высокая [CVE-2017-8715] - Средняя [CVE-2017-8716] - Средняя [CVE-2017-8717] - Высокая [CVE-2017-8718] - Высокая [CVE-2017-8719] - Средняя [CVE-2017-8720] - Высокая [CVE-2017-8723] - Средняя [CVE-2017-8724] - Средняя [CVE-2017-8726] - Средняя [CVE-2017-8727] - Высокая [CVE-2017-8728] - Высокая [CVE-2017-8729] - Высокая [CVE-2017-8731] - Высокая [CVE-2017-8733] - Средняя [CVE-2017-8734] - Высокая [CVE-2017-8735] - Средняя [CVE-2017-8736] - Средняя [CVE-2017-8737] - Высокая [CVE-2017-8738] - Высокая [CVE-2017-8739] - Средняя [CVE-2017-8740] - Высокая [CVE-2017-8741] - Высокая [CVE-2017-8747] - Высокая [CVE-2017-8748] - Высокая [CVE-2017-8749] - Высокая [CVE-2017-8750] - Высокая [CVE-2017-8751] - Высокая [CVE-2017-8752] - Высокая [CVE-2017-8753] - Высокая [CVE-2017-8754] - Средняя [CVE-2017-8755] - Высокая [CVE-2017-8756] - Высокая [CVE-2017-8757] - Высокая [CVE-2017-9511] - Высокая [CVE-2018-0598] - Высокая [CVE-2018-0741] - Средняя [CVE-2018-0749] - Высокая [CVE-2018-0755] - Средняя [CVE-2018-0758] - Высокая [CVE-2018-0760] - Средняя [CVE-2018-0761] - Средняя [CVE-2018-0762] - Высокая [CVE-2018-0763] - Низкая [CVE-2018-0766] - Средняя [CVE-2018-0767] - Средняя [CVE-2018-0768] - Высокая [CVE-2018-0769] - Высокая [CVE-2018-0770] - Высокая [CVE-2018-0771] - Средняя [CVE-2018-0772] - Высокая [CVE-2018-0773] - Высокая [CVE-2018-0774] - Высокая [CVE-2018-0775] - Высокая [CVE-2018-0776] - Высокая [CVE-2018-0777] - Высокая [CVE-2018-0778] - Высокая [CVE-2018-0780] - Средняя [CVE-2018-0781] - Высокая [CVE-2018-0800] - Средняя [CVE-2018-0803] - Средняя [CVE-2018-0811] - Средняя [CVE-2018-0813] - Средняя [CVE-2018-0814] - Средняя [CVE-2018-0815] - Высокая [CVE-2018-0816] - Высокая [CVE-2018-0817] - Высокая [CVE-2018-0824] - Высокая [CVE-2018-0833] - Средняя [CVE-2018-0834] - Высокая [CVE-2018-0835] - Высокая [CVE-2018-0836] - Высокая [CVE-2018-0837] - Высокая [CVE-2018-0838] - Высокая [CVE-2018-0839] - Средняя [CVE-2018-0840] - Высокая [CVE-2018-0847] - Средняя [CVE-2018-0855] - Средняя [CVE-2018-0856] - Высокая [CVE-2018-0857] - Высокая [CVE-2018-0859] - Высокая [CVE-2018-0860] - Высокая [CVE-2018-0861] - Высокая [CVE-2018-0866] - Высокая [CVE-2018-0868] - Высокая [CVE-2018-0872] - Высокая [CVE-2018-0873] - Высокая [CVE-2018-0874] - Высокая [CVE-2018-0876] - Высокая [CVE-2018-0878] - Низкая [CVE-2018-0879] - Высокая [CVE-2018-0881] - Высокая [CVE-2018-0883] - Высокая [CVE-2018-0885] - Средняя [CVE-2018-0886] - Высокая [CVE-2018-0888] - Средняя [CVE-2018-0889] - Высокая [CVE-2018-0891] - Средняя [CVE-2018-0893] - Высокая [CVE-2018-0894] - Средняя [CVE-2018-0895] - Средняя [CVE-2018-0896] - Средняя [CVE-2018-0897] - Средняя [CVE-2018-0898] - Средняя [CVE-2018-0899] - Средняя [CVE-2018-0900] - Средняя [CVE-2018-0901] - Средняя [CVE-2018-0904] - Средняя [CVE-2018-0926] - Средняя [CVE-2018-0927] - Средняя [CVE-2018-0929] - Средняя [CVE-2018-0930] - Высокая [CVE-2018-0931] - Высокая [CVE-2018-0932] - Средняя [CVE-2018-0933] - Высокая [CVE-2018-0934] - Высокая [CVE-2018-0935] - Высокая [CVE-2018-0936] - Высокая [CVE-2018-0937] - Высокая [CVE-2018-0939] - Средняя [CVE-2018-0942] - Низкая [CVE-2018-0952] - Высокая [CVE-2018-0986] - Высокая [CVE-2018-1003] - Высокая [CVE-2018-1009] - Высокая [CVE-2018-1010] - Высокая [CVE-2018-1012] - Высокая [CVE-2018-1013] - Высокая [CVE-2018-1015] - Высокая [CVE-2018-1016] - Высокая [CVE-2018-13399] - Высокая [CVE-2018-15408] - Высокая [CVE-2018-15409] - Высокая [CVE-2018-15410] - Высокая [CVE-2018-15411] - Высокая [CVE-2018-15412] - Высокая [CVE-2018-15413] - Высокая [CVE-2018-15414] - Высокая [CVE-2018-15415] - Высокая [CVE-2018-15416] - Высокая [CVE-2018-15417] - Высокая [CVE-2018-15418] - Высокая [CVE-2018-15419] - Высокая [CVE-2018-15420] - Высокая [CVE-2018-15421] - Высокая [CVE-2018-15422] - Высокая [CVE-2018-15431] - Высокая [CVE-2018-15437] - Средняя [CVE-2018-15490] - Высокая [CVE-2018-16794] - Высокая [CVE-2018-3700] - Средняя [CVE-2018-4858] - Высокая [CVE-2018-5440] - Критичная [CVE-2018-6661] - Высокая [CVE-2018-6664] - Высокая [CVE-2018-6674] - Низкая [CVE-2018-6687] - Средняя [CVE-2018-6690] - Высокая [CVE-2018-6700] - Высокая [CVE-2018-6755] - Высокая [CVE-2018-6756] - Высокая [CVE-2018-6757] - Высокая [CVE-2018-6765] - Высокая [CVE-2018-7249] - Высокая [CVE-2018-7250] - Средняя [CVE-2018-8116] - Средняя [CVE-2018-8218] - Высокая [CVE-2018-8253] - Средняя [CVE-2018-8256] - Высокая [CVE-2018-8307] - Средняя [CVE-2018-8332] - Высокая [CVE-2018-8333] - Высокая [CVE-2018-8335] - Высокая [CVE-2018-8344] - Высокая [CVE-2018-8345] - Высокая [CVE-2018-8346] - Высокая [CVE-2018-8347] - Высокая [CVE-2018-8349] - Высокая [CVE-2018-8350] - Высокая [CVE-2018-8392] - Высокая [CVE-2018-8393] - Высокая [CVE-2018-8407] - Средняя [CVE-2018-8415] - Высокая [CVE-2018-8417] - Средняя [CVE-2018-8420] - Высокая [CVE-2018-8423] - Высокая [CVE-2018-8427] - Средняя [CVE-2018-8432] - Высокая [CVE-2018-8433] - Средняя [CVE-2018-8436] - Средняя [CVE-2018-8437] - Средняя [CVE-2018-8438] - Средняя [CVE-2018-8444] - Средняя [CVE-2018-8471] - Высокая [CVE-2018-8494] - Высокая [CVE-2018-8506] - Средняя [CVE-2018-8547] - Средняя [CVE-2018-8553] - Высокая [CVE-2018-8599] - Высокая [CVE-2018-8634] - Высокая [CVE-2018-8853] - Высокая [CVE-2019-0232] - Высокая [CVE-2019-0543] - Высокая [CVE-2019-0555] - Высокая [CVE-2019-0630] - Высокая [CVE-2019-0633] - Высокая [CVE-2019-0690] - Средняя [CVE-2019-0695] - Средняя [CVE-2019-0701] - Средняя [CVE-2019-0710] - Средняя [CVE-2019-0711] - Средняя [CVE-2019-0712] - Средняя [CVE-2019-0713] - Средняя [CVE-2019-0714] - Средняя [CVE-2019-0715] - Средняя [CVE-2019-0717] - Средняя [CVE-2019-0718] - Средняя [CVE-2019-0723] - Средняя [CVE-2019-0734] - Высокая [CVE-2019-0766] - Высокая [CVE-2019-0885] - Высокая [CVE-2019-0928] - Средняя [CVE-2019-0936] - Высокая [CVE-2019-0966] - Средняя [CVE-2019-1019] - Высокая [CVE-2019-1040] - Средняя [CVE-2019-1074] - Средняя [CVE-2019-1078] - Средняя [CVE-2019-1082] - Высокая [CVE-2019-1089] - Высокая [CVE-2019-1144] - Высокая [CVE-2019-1145] - Высокая [CVE-2019-1148] - Средняя [CVE-2019-1149] - Высокая [CVE-2019-1150] - Высокая [CVE-2019-1151] - Высокая [CVE-2019-1152] - Высокая [CVE-2019-1153] - Средняя [CVE-2019-1166] - Средняя [CVE-2019-1168] - Высокая [CVE-2019-11684] - Критичная [CVE-2019-1172] - Средняя [CVE-2019-1177] - Высокая [CVE-2019-1188] - Высокая [CVE-2019-1198] - Высокая [CVE-2019-1270] - Средняя [CVE-2019-1280] - Высокая [CVE-2019-1309] - Средняя [CVE-2019-1310] - Средняя [CVE-2019-1316] - Высокая [CVE-2019-1317] - Высокая [CVE-2019-1318] - Средняя [CVE-2019-1320] - Высокая [CVE-2019-1321] - Высокая [CVE-2019-1322] - Высокая [CVE-2019-1323] - Высокая [CVE-2019-1336] - Высокая [CVE-2019-1338] - Средняя [CVE-2019-1340] - Высокая [CVE-2019-1381] - Средняя [CVE-2019-1384] - Критичная [CVE-2019-1399] - Средняя [CVE-2019-1409] - Средняя [CVE-2019-1419] - Высокая [CVE-2019-1430] - Высокая [CVE-2019-1456] - Высокая [CVE-2019-1484] - Высокая [CVE-2019-15162] - Средняя [CVE-2019-15283] - Высокая [CVE-2019-15284] - Высокая [CVE-2019-15285] - Высокая [CVE-2019-15286] - Высокая [CVE-2019-15287] - Высокая [CVE-2019-1637] - Высокая [CVE-2019-1638] - Высокая [CVE-2019-1639] - Высокая [CVE-2019-1640] - Высокая [CVE-2019-1641] - Высокая [CVE-2019-1771] - Высокая [CVE-2019-1772] - Высокая [CVE-2019-1773] - Высокая [CVE-2019-18232] - Высокая [CVE-2019-18631] - Высокая [CVE-2019-18913] - Средняя [CVE-2019-1924] - Высокая [CVE-2019-1925] - Высокая [CVE-2019-1926] - Высокая [CVE-2019-1927] - Высокая [CVE-2019-1928] - Высокая [CVE-2019-1929] - Высокая [CVE-2019-19363] - Высокая [CVE-2019-20406] - Высокая [CVE-2019-2390] - Высокая [CVE-2019-3582] - Высокая [CVE-2019-3585] - Высокая [CVE-2019-3587] - Средняя [CVE-2019-3588] - Средняя [CVE-2019-3593] - Высокая [CVE-2019-3610] - Средняя [CVE-2019-3646] - Средняя [CVE-2019-3648] - Средняя [CVE-2019-3654] - Высокая [CVE-2019-3667] - Высокая [CVE-2019-3880] - Средняя [CVE-2019-4732] - Средняя [CVE-2019-6265] - Высокая [CVE-2019-6266] - Критичная [CVE-2019-9510] - Высокая [CVE-2020-0616] - Средняя [CVE-2020-0622] - Средняя [CVE-2020-0635] - Высокая [CVE-2020-0641] - Высокая [CVE-2020-0644] - Высокая [CVE-2020-0661] - Средняя [CVE-2020-0684] - Высокая [CVE-2020-0687] - Высокая [CVE-2020-0729] - Высокая [CVE-2020-0751] - Средняя [CVE-2020-0796] - Критичная [CVE-2020-0799] - Высокая [CVE-2020-0890] - Средняя [CVE-2020-0904] - Средняя [CVE-2020-0921] - Средняя [CVE-2020-0922] - Высокая [CVE-2020-0938] - Высокая [CVE-2020-0965] - Высокая [CVE-2020-0982] - Средняя [CVE-2020-0987] - Средняя [CVE-2020-1005] - Средняя [CVE-2020-1009] - Высокая [CVE-2020-1010] - Высокая [CVE-2020-1013] - Высокая [CVE-2020-1014] - Высокая [CVE-2020-1018] - Высокая [CVE-2020-1020] - Высокая [CVE-2020-1068] - Высокая [CVE-2020-1079] - Высокая [CVE-2020-1083] - Средняя [CVE-2020-1118] - Высокая [CVE-2020-1129] - Высокая [CVE-2020-1160] - Средняя [CVE-2020-1163] - Высокая [CVE-2020-1170] - Высокая [CVE-2020-1206] - Высокая [CVE-2020-1243] - Высокая [CVE-2020-1281] - Высокая [CVE-2020-1284] - Средняя [CVE-2020-1299] - Высокая [CVE-2020-1300] - Высокая [CVE-2020-1301] - Высокая [CVE-2020-13162] - Высокая [CVE-2020-1319] - Высокая [CVE-2020-1351] - Средняя [CVE-2020-1383] - Средняя [CVE-2020-1408] - Высокая [CVE-2020-1421] - Высокая [CVE-2020-1425] - Высокая [CVE-2020-1457] - Высокая [CVE-2020-1471] - Высокая [CVE-2020-1507] - Высокая [CVE-2020-15145] - Высокая [CVE-2020-1560] - Высокая [CVE-2020-1574] - Высокая [CVE-2020-1585] - Высокая [CVE-2020-16877] - Высокая [CVE-2020-16910] - Средняя [CVE-2020-17022] - Высокая [CVE-2020-17162] - Высокая [CVE-2020-24556] - Высокая [CVE-2020-24557] - Высокая [CVE-2020-24562] - Высокая [CVE-2020-25182] - Средняя [CVE-2020-3127] - Высокая [CVE-2020-3128] - Высокая [CVE-2020-3194] - Высокая [CVE-2020-3319] - Низкая [CVE-2020-3321] - Низкая [CVE-2020-3322] - Низкая [CVE-2020-36233] - Высокая [CVE-2020-36603] - Средняя [CVE-2020-4739] - Высокая [CVE-2020-4767] - Высокая [CVE-2020-5384] - Высокая [CVE-2020-7205] - Средняя [CVE-2020-7299] - Средняя [CVE-2020-7320] - Высокая [CVE-2020-7335] - Высокая [CVE-2021-1372] - Средняя [CVE-2021-1710] - Высокая [CVE-2021-21513] - Критичная [CVE-2021-21706] - Средняя [CVE-2021-24076] - Средняя [CVE-2021-24081] - Высокая [CVE-2021-26432] - Критичная [CVE-2021-26433] - Высокая [CVE-2021-26881] - Высокая [CVE-2021-26887] - Высокая [CVE-2021-28317] - Средняя [CVE-2021-31184] - Средняя [CVE-2021-32022] - Средняя [CVE-2021-34439] - Высокая [CVE-2021-34441] - Высокая [CVE-2021-34471] - Высокая [CVE-2021-34503] - Высокая [CVE-2021-34579] - Высокая [CVE-2021-35211] - Критичная [CVE-2021-36745] - Критичная [CVE-2021-36926] - Высокая [CVE-2021-36932] - Высокая [CVE-2021-36933] - Высокая [CVE-2021-38505] - Средняя [CVE-2021-38634] - Высокая [CVE-2021-39032] - Средняя [CVE-2021-40828] - Высокая [CVE-2021-41065] - Высокая [CVE-2021-41330] - Высокая [CVE-2021-42275] - Высокая [CVE-2021-42276] - Высокая [CVE-2022-1794] - Средняя [CVE-2022-21606] - Средняя [CVE-2022-21993] - Высокая [CVE-2022-22516] - Высокая [CVE-2022-22765] - Высокая [CVE-2022-22782] - Высокая [CVE-2022-23235] - Средняя [CVE-2022-23239] - Средняя [CVE-2022-23240] - Средняя [CVE-2022-23609] - Критичная [CVE-2022-23611] - Критичная [CVE-2022-23678] - Средняя [CVE-2022-24765] - Высокая [CVE-2022-24826] - Высокая [CVE-2022-27167] - Высокая [CVE-2022-27608] - Средняя [CVE-2022-27609] - Средняя [CVE-2022-29105] - Высокая [CVE-2022-30190] - Высокая [CVE-2022-32230] - Высокая [CVE-2022-34006] - Высокая [CVE-2022-34478] - Средняя [CVE-2022-34713] - Высокая [CVE-2022-35743] - Высокая [CVE-2022-36670] - Средняя [CVE-2022-37771] - Средняя [CVE-2022-37971] - Высокая [CVE-2022-39327] - Критичная [CVE-2022-40263] - Высокая [CVE-2022-41120] - Высокая [CVE-2022-44704] - Высокая [CVE-2022-45141] - Критичная [CVE-2023-1587] - Средняя [CVE-2023-22880] - Высокая [CVE-2023-28005] - Средняя [CVE-2023-28290] - Средняя [CVE-2023-28297] - Высокая [CVE-2023-31222] - Высокая [CVE-2023-34355] - Высокая [CVE-2023-38175] - Высокая [CVE-2023-38402] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2000-0771] "Microsoft Windows 2000 allows local users to cause a denial of service by corrupting the local security policy via malformed RPC traffic, aka the ""Local Security Policy Corruption"" vulnerability."  
  
[CVE-2001-0509] Vulnerabilities in RPC servers in (1) Microsoft Exchange Server 2000 and earlier, (2) Microsoft SQL Server 2000 and earlier, (3) Windows NT 4.0, and (4) Windows 2000 allow remote attackers to cause a denial of service via malformed inputs.  
  
[CVE-2002-1140] "The Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service (service hang) via malformed packet fragments, aka ""Improper parameter size check leading to denial of service."""  
  
[CVE-2002-1141] "An input validation error in the Sun Microsystems RPC library Services for Unix 3.0 Interix SD, as implemented on Microsoft Windows NT4, 2000, and XP, allows remote attackers to cause a denial of service via malformed fragmented RPC client packets, aka ""Denial of service by sending an invalid RPC request."""  
  
[CVE-2003-0003] Buffer overflow in the RPC Locator service for Microsoft Windows NT 4.0, Windows NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows local users to execute arbitrary code via an RPC call to the service containing certain parameter information.  
  
[CVE-2003-0352] Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms.  
  
[CVE-2003-0807] Buffer overflow in the COM Internet Services and in the RPC over HTTP Proxy components for Microsoft Windows NT Server 4.0, NT 4.0 Terminal Server Edition, 2000, XP, and Server 2003 allows remote attackers to cause a denial of service via a crafted request.  
  
[CVE-2004-0116] An Activation function in the RPCSS Service involved with DCOM activation for Microsoft Windows 2000, XP, and 2003 allows remote attackers to cause a denial of service (memory consumption) via an activation request with a large length field.  
  
[CVE-2004-0124] "The DCOM RPC interface for Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to cause network communications via an ""alter context"" call that contains additional data, aka the ""Object Identity Vulnerability."""  
  
[CVE-2004-0569] The RPC Runtime Library for Microsoft Windows NT 4.0 allows remote attackers to read active memory or cause a denial of service (system crash) via a malicious message, possibly related to improper length values.  
  
[CVE-2005-3644] PNP\_GetDeviceList (upnp\_getdevicelist) in UPnP for Microsoft Windows 2000 SP4 and earlier, and possibly Windows XP SP1 and earlier, allows remote attackers to cause a denial of service (memory consumption) via a DCE RPC request that specifies a large output buffer size, a variant of CVE-2006-6296, and a different vulnerability than CVE-2005-2120.  
  
[CVE-2006-0013] Buffer overflow in the Web Client service (WebClnt.dll) for Microsoft Windows XP SP1 and SP2, and Server 2003 up to SP1, allows remote authenticated users or Guests to execute arbitrary code via crafted RPC requests, a different vulnerability than CVE-2005-1207.  
  
[CVE-2006-0034] Heap-based buffer overflow in the CRpcIoManagerServer::BuildContext function in msdtcprx.dll for Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0 and Windows 2000 SP2 and SP3 allows remote attackers to execute arbitrary code via a long fifth argument to the BuildContextW or BuildContext opcode, which triggers a bug in the NdrAllocate function, aka the MSDTC Invalid Memory Access Vulnerability.  
  
[CVE-2006-2370] "Buffer overflow in the Routing and Remote Access service (RRAS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted ""RPC related requests,"" aka the ""RRAS Memory Corruption Vulnerability."""  
  
[CVE-2006-2371] "Buffer overflow in the Remote Access Connection Manager service (RASMAN) service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote unauthenticated or authenticated attackers to execute arbitrary code via certain crafted ""RPC related requests,"" that lead to registry corruption and stack corruption, aka the ""RASMAN Registry Corruption Vulnerability."""  
  
[CVE-2006-2380] "Microsoft Windows 2000 SP4 does not properly validate an RPC server during mutual authentication over SSL, which allows remote attackers to spoof an RPC server, aka the ""RPC Mutual Authentication Vulnerability."""  
  
[CVE-2006-3439] Buffer overflow in the Server Service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers, including anonymous users, to execute arbitrary code via a crafted RPC message, a different vulnerability than CVE-2006-1314.  
  
[CVE-2006-4691] Stack-based buffer overflow in the NetpManageIPCConnect function in the Workstation service (wkssvc.dll) in Microsoft Windows 2000 SP4 and XP SP2 allows remote attackers to execute arbitrary code via NetrJoinDomain2 RPC messages with a long hostname.  
  
[CVE-2006-6296] The RpcGetPrinterData function in the Print Spooler (spoolsv.exe) service in Microsoft Windows 2000 SP4 and earlier, and possibly Windows XP SP1 and earlier, allows remote attackers to cause a denial of service (memory consumption) via an RPC request that specifies a large 'offered' value (output buffer size), a variant of CVE-2005-3644.  
  
[CVE-2006-6723] The Workstation service in Microsoft Windows 2000 SP4 and XP SP2 allows remote attackers to cause a denial of service (memory consumption) via a large maxlen value in an NetrWkstaUserEnum RPC request.  
  
[CVE-2007-1748] Stack-based buffer overflow in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 Server SP 4, Server 2003 SP 1, and Server 2003 SP 2 allows remote attackers to execute arbitrary code via a long zone name containing character constants represented by escape sequences.  
  
[CVE-2007-2228] rpcrt4.dll (aka the RPC runtime library) in Microsoft Windows XP SP2, XP Professional x64 Edition, Server 2003 SP1 and SP2, Server 2003 x64 Edition and x64 Edition SP2, and Vista and Vista x64 Edition allows remote attackers to cause a denial of service (RPCSS service stop and system restart) via an RPC request that uses NTLMSSP PACKET authentication with a zero-valued verification trailer signature, which triggers an invalid dereference. NOTE: this also affects Windows 2000 SP4, although the impact is an information leak.  
  
[CVE-2007-3039] Stack-based buffer overflow in the Microsoft Message Queuing (MSMQ) service in Microsoft Windows 2000 Server SP4, Windows 2000 Professional SP4, and Windows XP SP2 allows attackers to execute arbitrary code via a long string in an opnum 0x06 RPC call to port 2103. NOTE: this is remotely exploitable on Windows 2000 Server.  
  
[CVE-2008-3479] "Heap-based buffer overflow in the Microsoft Message Queuing (MSMQ) service (mqsvc.exe) in Microsoft Windows 2000 SP4 allows remote attackers to read memory contents and execute arbitrary code via a crafted RPC call, related to improper processing of parameters to string APIs, aka ""Message Queuing Service Remote Code Execution Vulnerability."""  
  
[CVE-2008-4114] "srv.sys in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via an SMB WRITE\_ANDX packet with an offset that is inconsistent with the packet size, related to ""insufficiently validating the buffer size,"" as demonstrated by a request to the \PIPE\lsarpc named pipe, aka ""SMB Validation Denial of Service Vulnerability."""  
  
[CVE-2008-4250] "The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka ""Server Service Vulnerability."""  
  
[CVE-2009-0079] "The RPCSS service in Microsoft Windows XP SP2 and SP3 and Server 2003 SP1 and SP2 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka ""Windows RPCSS Service Isolation Vulnerability."""  
  
[CVE-2009-0228] "Stack-based buffer overflow in the EnumeratePrintShares function in Windows Print Spooler Service (win32spl.dll) in Microsoft Windows 2000 SP4 allows remote printer servers to execute arbitrary code via a crafted ShareName in a response to an RPC request, related to ""printing data structures,"" aka ""Buffer Overflow in Print Spooler Vulnerability."""  
  
[CVE-2009-0230] "The Windows Print Spooler in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 allows remote authenticated users to gain privileges via a crafted RPC message that triggers loading of a DLL file from an arbitrary directory, aka ""Print Spooler Load Library Vulnerability."""  
  
[CVE-2009-0568] "The RPC Marshalling Engine (aka NDR) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly maintain its internal state, which allows remote attackers to overwrite arbitrary memory locations via a crafted RPC message that triggers incorrect pointer reading, related to ""IDL interfaces containing a non-conformant varying array"" and FC\_SMVARRAY, FC\_LGVARRAY, FC\_VARIABLE\_REPEAT, and FC\_VARIABLE\_OFFSET, aka ""RPC Marshalling Engine Vulnerability."""  
  
[CVE-2009-1544] "Double free vulnerability in the Workstation service in Microsoft Windows allows remote authenticated users to gain privileges via a crafted RPC message to a Windows XP SP2 or SP3 or Server 2003 SP2 system, or cause a denial of service via a crafted RPC message to a Vista Gold, SP1, or SP2 or Server 2008 Gold or SP2 system, aka ""Workstation Service Memory Corruption Vulnerability."""  
  
[CVE-2009-2523] "The License Logging Server (llssrv.exe) in Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via an RPC message containing a string without a null terminator, which triggers a heap-based buffer overflow in the LlsrLicenseRequestW method, aka ""License Logging Server Heap Overflow Vulnerability."""  
  
[CVE-2010-2567] "The RPC client implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly allocate memory during the parsing of responses, which allows remote RPC servers and man-in-the-middle attackers to execute arbitrary code via a malformed response, aka ""RPC Memory Corruption Vulnerability."""  
  
[CVE-2010-2729] "The Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when printer sharing is enabled, does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code, by sending a crafted print request over RPC, as exploited in the wild in September 2010, aka ""Print Spooler Service Impersonation Vulnerability."""  
  
[CVE-2010-2742] "The Netlogon RPC Service in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, and R2, when the domain controller role is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via a crafted RPC packet, aka ""Netlogon RPC Null dereference DOS Vulnerability."""  
  
[CVE-2010-3139] Untrusted search path vulnerability in Microsoft Windows Progman Group Converter (grpconv.exe) allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse imm.dll that is located in the same folder as a .grp file.  
  
[CVE-2010-3222] "Stack-based buffer overflow in the Remote Procedure Call Subsystem (RPCSS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted LPC message that requests an LRPC connection from an LPC server to a client, aka ""LPC Message Buffer Overrun Vulnerability."""  
  
[CVE-2013-3175] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a malformed asynchronous RPC request, aka ""Remote Procedure Call Vulnerability."""  
  
[CVE-2013-3878] "Stack-based buffer overflow in the LRPC client in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges by operating an LRPC server that sends a crafted LPC port message, aka ""LRPC Client Buffer Overrun Vulnerability."""  
  
[CVE-2014-0316] "Memory leak in the Local RPC (LRPC) server implementation in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (memory consumption) and bypass the ASLR protection mechanism via a crafted client that sends messages with an invalid data view, aka ""LRPC ASLR Bypass Vulnerability."""  
  
[CVE-2015-2370] "The authentication implementation in the RPC subsystem in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not prevent DCE/RPC connection reflection, which allows local users to gain privileges via a crafted application, aka ""Windows RPC Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0128] "The SAM and LSAD protocol implementations in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 do not properly establish an RPC channel, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka ""Windows SAM and LSAD Downgrade Vulnerability"" or ""BADLOCK."""  
  
[CVE-2016-0178] "The RPC NDR Engine in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles free operations, which allows remote attackers to execute arbitrary code via malformed RPC requests, aka ""RPC Network Data Representation Engine Elevation of Privilege Vulnerability."""  
  
[CVE-2020-1113] A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.  
  
[CVE-1999-0012] Some web servers under Microsoft Windows allow remote attackers to bypass access restrictions for files with long file names.  
  
[CVE-1999-0227] Access violation in LSASS.EXE (LSA/LSARPC) program in Windows NT allows a denial of service.  
  
[CVE-1999-0228] Denial of service in RPCSS.EXE program (RPC Locator) in Windows NT.  
  
[CVE-1999-0288] The WINS server in Microsoft Windows NT 4.0 before SP4 allows remote attackers to cause a denial of service (process termination) via invalid UDP frames to port 137 (NETBIOS Name Service), as demonstrated via a flood of random packets.  
  
[CVE-1999-0386] Microsoft Personal Web Server and FrontPage Personal Web Server in some Windows systems allows a remote attacker to read files on the server by using a nonstandard URL.  
  
[CVE-1999-0681] Buffer overflow in Microsoft FrontPage Server Extensions (PWS) 3.0.2.926 on Windows 95, and possibly other versions, allows remote attackers to cause a denial of service via a long URL.  
  
[CVE-1999-0749] Buffer overflow in Microsoft Telnet client in Windows 95 and Windows 98 via a malformed Telnet argument.  
  
[CVE-1999-0969] The Windows NT RPC service allows remote attackers to conduct a denial of service using spoofed malformed RPC packets which generate an error message that is sent to the spoofed host, potentially setting up a loop, aka Snork.  
  
[CVE-1999-1127] "Windows NT 4.0 does not properly shut down invalid named pipe RPC connections, which allows remote attackers to cause a denial of service (resource exhaustion) via a series of connections containing malformed data, aka the ""Named Pipes Over RPC"" vulnerability."  
  
[CVE-1999-1291] TCP/IP implementation in Microsoft Windows 95, Windows NT 4.0, and possibly others, allows remote attackers to reset connections by forcing a reset (RST) via a PSH ACK or other means, obtaining the target's last sequence number from the resulting packet, then spoofing a reset to the target.  
  
[CVE-2000-0089] "The rdisk utility in Microsoft Terminal Server Edition and Windows NT 4.0 stores registry hive information in a temporary file with permissions that allow local users to read it, aka the ""RDISK Registry Enumeration File"" vulnerability."  
  
[CVE-2000-0168] "Microsoft Windows 9x operating systems allow an attacker to cause a denial of service via a pathname that includes file device names, aka the ""DOS Device in Path Name"" vulnerability."  
  
[CVE-2000-0216] Microsoft email clients in Outlook, Exchange, and Windows Messaging automatically respond to Read Receipt and Delivery Receipt tags, which could allow an attacker to flood a mail system with responses by forging a Read Receipt request that is redirected to a large distribution list.  
  
[CVE-2000-0228] "Microsoft Windows Media License Manager allows remote attackers to cause a denial of service by sending a malformed request that causes the manager to halt, aka the ""Malformed Media License Request"" Vulnerability."  
  
[CVE-2000-0331] "Buffer overflow in Microsoft command processor (CMD.EXE) for Windows NT and Windows 2000 allows a local user to cause a denial of service via a long environment variable, aka the ""Malformed Environment Variable"" vulnerability."  
  
[CVE-2000-0495] "Microsoft Windows Media Encoder allows remote attackers to cause a denial of service via a malformed request, aka the ""Malformed Windows Media Encoder Request"" vulnerability."  
  
[CVE-2000-0544] Windows NT and Windows 2000 hosts allow a remote attacker to cause a denial of service via malformed DCE/RPC SMBwriteX requests that contain an invalid data length.  
  
[CVE-2000-0653] "Microsoft Outlook Express allows remote attackers to monitor a user's email by creating a persistent browser link to the Outlook Express windows, aka the ""Persistent Mail-Browser Link"" vulnerability."  
  
[CVE-2000-0742] "The IPX protocol implementation in Microsoft Windows 95 and 98 allows remote attackers to cause a denial of service by sending a ping packet with a source IP address that is a broadcast address, aka the ""Malformed IPX Ping Packet"" vulnerability."  
  
[CVE-2000-0790] The web-based folder display capability in Microsoft Internet Explorer 5.5 on Windows 98 allows local users to insert Trojan horse programs by modifying the Folder.htt file and using the InvokeVerb method in the ShellDefView ActiveX control to specify a default execute option for the first file that is listed in the folder.  
  
[CVE-2000-0849] "Race condition in Microsoft Windows Media server allows remote attackers to cause a denial of service in the Windows Media Unicast Service via a malformed request, aka the ""Unicast Service Race Condition"" vulnerability."  
  
[CVE-2000-0858] "Vulnerability in Microsoft Windows NT 4.0 allows remote attackers to cause a denial of service in IIS by sending it a series of malformed requests which cause INETINFO.EXE to fail, aka the ""Invalid URL"" vulnerability."  
  
[CVE-2000-0929] "Microsoft Windows Media Player 7 allows attackers to cause a denial of service in RTF-enabled email clients via an embedded OCX control that is not closed properly, aka the ""OCX Attachment"" vulnerability."  
  
[CVE-2000-0942] "The CiWebHitsFile component in Microsoft Indexing Services for Windows 2000 allows remote attackers to conduct a cross site scripting (CSS) attack via a CiRestriction parameter in a .htw request, aka the ""Indexing Services Cross Site Scripting"" vulnerability."  
  
[CVE-2000-1079] Interactions between the CIFS Browser Protocol and NetBIOS as implemented in Microsoft Windows 95, 98, NT, and 2000 allow remote attackers to modify dynamic NetBIOS name cache entries via a spoofed Browse Frame Request in a unicast or UDP broadcast datagram.  
  
[CVE-2000-1112] "Microsoft Windows Media Player 7 executes scripts in custom skin (.WMS) files, which could allow remote attackers to gain privileges via a skin that contains a malicious script, aka the "".WMS Script Execution"" vulnerability."  
  
[CVE-2000-1113] "Buffer overflow in Microsoft Windows Media Player allows remote attackers to execute arbitrary commands via a malformed Active Stream Redirector (.ASX) file, aka the "".ASX Buffer Overrun"" vulnerability."  
  
[CVE-2000-1217] "Microsoft Windows 2000 before Service Pack 2 (SP2), when running in a non-Windows 2000 domain and using NTLM authentication, and when credentials of an account are locally cached, allows local users to bypass account lockout policies and make an unlimited number of login attempts, aka the ""Domain Account Lockout"" vulnerability."  
  
[CVE-2000-1218] The default configuration for the domain name resolver for Microsoft Windows 98, NT 4.0, 2000, and XP sets the QueryIpMatching parameter to 0, which causes Windows to accept DNS updates from hosts that it did not query, which allows remote attackers to poison the DNS cache.  
  
[CVE-2001-0003] "Web Extender Client (WEC) in Microsoft Office 2000, Windows 2000, and Windows Me does not properly process Internet Explorer security settings for NTLM authentication, which allows attackers to obtain NTLM credentials and possibly obtain the password, aka the ""Web Client NTLM Authentication"" vulnerability."  
  
[CVE-2001-0047] "The default permissions for the MTS Package Administration registry key in Windows NT 4.0 allows local users to install or modify arbitrary Microsoft Transaction Server (MTS) packages and gain privileges, aka one of the ""Registry Permissions"" vulnerabilities."  
  
[CVE-2001-0242] "Buffer overflows in Microsoft Windows Media Player 7 and earlier allow remote attackers to execute arbitrary commands via (1) a long version tag in an .ASX file, or (2) a long banner tag, a variant of the "".ASX Buffer Overrun"" vulnerability as discussed in MS:MS00-090."  
  
[CVE-2001-0245] "Microsoft Index Server 2.0 in Windows NT 4.0, and Indexing Service in Windows 2000, allows remote attackers to read server-side include files via a malformed search request, aka a new variant of the ""Malformed Hit-Highlighting"" vulnerability."  
  
[CVE-2001-0261] Microsoft Windows 2000 Encrypted File System does not properly destroy backups of files that are encrypted, which allows a local attacker to recover the text of encrypted files.  
  
[CVE-2001-0345] Microsoft Windows 2000 telnet service allows attackers to prevent idle Telnet sessions from timing out, causing a denial of service by creating a large number of idle sessions.  
  
[CVE-2001-0346] Handle leak in Microsoft Windows 2000 telnet service allows attackers to cause a denial of service by starting a large number of sessions and terminating them.  
  
[CVE-2001-0347] Information disclosure vulnerability in Microsoft Windows 2000 telnet service allows remote attackers to determine the existence of user accounts such as Guest, or log in to the server without specifying the domain name, via a malformed userid.  
  
[CVE-2001-0348] Microsoft Windows 2000 telnet service allows attackers to cause a denial of service (crash) via a long logon command that contains a backspace.  
  
[CVE-2001-0349] Microsoft Windows 2000 telnet service creates named pipes with predictable names and does not properly verify them, which allows local users to execute arbitrary commands by creating a named pipe with the predictable name and associating a malicious program with it, the first of two variants of this vulnerability.  
  
[CVE-2001-0350] Microsoft Windows 2000 telnet service creates named pipes with predictable names and does not properly verify them, which allows local users to execute arbitrary commands by creating a named pipe with the predictable name and associating a malicious program with it, the second of two variants of this vulnerability.  
  
[CVE-2001-0351] Microsoft Windows 2000 telnet service allows a local user to make a certain system call that allows the user to terminate a Telnet session and cause a denial of service.  
  
[CVE-2001-0504] Vulnerability in authentication process for SMTP service in Microsoft Windows 2000 allows remote attackers to use incorrect credentials to gain privileges and conduct activities such as mail relaying.  
  
[CVE-2001-0541] Buffer overflow in Microsoft Windows Media Player 7.1 and earlier allows remote attackers to execute arbitrary commands via a malformed Windows Media Station (.NSC) file.  
  
[CVE-2001-0662] RPC endpoint mapper in Windows NT 4.0 allows remote attackers to cause a denial of service (loss of RPC services) via a malformed request.  
  
[CVE-2001-0719] Buffer overflow in Microsoft Windows Media Player 6.4 allows remote attackers to execute arbitrary code via a malformed Advanced Streaming Format (ASF) file.  
  
[CVE-2001-0909] Buffer overflow in helpctr.exe program in Microsoft Help Center for Windows XP allows remote attackers to execute arbitrary code via a long hcp: URL.  
  
[CVE-2001-1055] The Microsoft Windows network stack allows remote attackers to cause a denial of service (CPU consumption) via a flood of malformed ARP request packets with random source IP and MAC addresses, as demonstrated by ARPNuke.  
  
[CVE-2001-1200] Microsoft Windows XP allows local users to bypass a locked screen and run certain programs that are associated with Hot Keys.  
  
[CVE-2001-1451] Memory leak in the SNMP LAN Manager (LANMAN) MIB extension for Microsoft Windows 2000 before SP3, when the Print Spooler is not running, allows remote attackers to cause a denial of service (memory consumption) via a large number of GET or GETNEXT requests.  
  
[CVE-2002-0018] In Microsoft Windows NT and Windows 2000, a trusting domain that receives authorization information from a trusted domain does not verify that the trusted domain is authoritative for all listed SIDs, which allows remote attackers to gain Domain Administrator privileges on the trusting domain by injecting SIDs from untrusted domains into the authorization data that comes from from the trusted domain.  
  
[CVE-2002-0034] The Microsoft CONVERT.EXE program, when used on Windows 2000 and Windows XP systems, does not apply the default NTFS permissions when converting a FAT32 file system, which could cause the conversion to produce a file system with less secure permissions than expected.  
  
[CVE-2002-0054] SMTP service in (1) Microsoft Windows 2000 and (2) Internet Mail Connector (IMC) in Exchange Server 5.5 does not properly handle responses to NTLM authentication, which allows remote attackers to perform mail relaying via an SMTP AUTH command using null session credentials.  
  
[CVE-2002-0055] SMTP service in Microsoft Windows 2000, Windows XP Professional, and Exchange 2000 allows remote attackers to cause a denial of service via a command with a malformed data transfer (BDAT) request.  
  
[CVE-2002-0136] Microsoft Internet Explorer 5.5 on Windows 98 allows remote web pages to cause a denial of service (hang) via extremely long values for form fields such as INPUT and TEXTAREA, which can be automatically filled via Javascript.  
  
[CVE-2002-0151] Buffer overflow in Multiple UNC Provider (MUP) in Microsoft Windows operating systems allows local users to cause a denial of service or possibly gain SYSTEM privileges via a long UNC request.  
  
[CVE-2002-0224] The MSDTC (Microsoft Distributed Transaction Service Coordinator) for Microsoft Windows 2000, Microsoft IIS 5.0 and SQL Server 6.5 through SQL 2000 0.0 allows remote attackers to cause a denial of service (crash or hang) via malformed (random) input.  
  
[CVE-2002-0370] Buffer overflow in the ZIP capability for multiple products allows remote attackers to cause a denial of service or execute arbitrary code via ZIP files containing entries with long filenames, including (1) Microsoft Windows 98 with Plus! Pack, (2) Windows XP, (3) Windows ME, (4) Lotus Notes R4 through R6 (pre-gold), (5) Verity KeyView, and (6) Stuffit Expander before 7.0.  
  
[CVE-2002-0372] "Microsoft Windows Media Player versions 6.4 and 7.1 and Media Player for Windows XP allow remote attackers to bypass Internet Explorer's (IE) security mechanisms and run code via an executable .wma media file with a license installation requirement stored in the IE cache, aka the ""Cache Path Disclosure via Windows Media Player""."  
  
[CVE-2002-0373] "The Windows Media Device Manager (WMDM) Service in Microsoft Windows Media Player 7.1 on Windows 2000 systems allows local users to obtain LocalSystem rights via a program that calls the WMDM service to connect to an invalid local storage device, aka ""Privilege Elevation through Windows Media Device Manager Service""."  
  
[CVE-2002-0443] Microsoft Windows 2000 allows local users to bypass the policy that prohibits reusing old passwords by changing the current password before it expires, which does not enable the check for previous passwords.  
  
[CVE-2002-0444] Microsoft Windows 2000 running the Terminal Server 90-day trial version, and possibly other versions, does not apply group policies to incoming users when the number of connections to the SYSVOL share exceeds the maximum, e.g. with a maximum number of licenses, which can allow remote authenticated users to bypass group policies.  
  
[CVE-2002-0597] LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445.  
  
[CVE-2002-0615] "The Windows Media Active Playlist in Microsoft Windows Media Player 7.1 stores information in a well known location on the local file system, allowing attackers to execute HTML scripts in the Local Computer zone, aka ""Media Playback Script Invocation""."  
  
[CVE-2002-0616] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code by attaching an inline macro to an object within an Excel workbook, aka the ""Excel Inline Macros Vulnerability."""  
  
[CVE-2002-0617] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code by creating a hyperlink on a drawing shape in a source workbook that points to a destination workbook containing an autoexecute macro, aka ""Hyperlinked Excel Workbook Macro Bypass."""  
  
[CVE-2002-0618] "The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code in the Local Computer zone by embedding HTML scripts within an Excel workbook that contains an XSL stylesheet, aka ""Excel XSL Stylesheet Script Execution""."  
  
[CVE-2002-0619] "The Mail Merge Tool in Microsoft Word 2002 for Windows, when Microsoft Access is present on a system, allows remote attackers to execute Visual Basic (VBA) scripts within a mail merge document that is saved in HTML format, aka a ""Variant of MS00-071, Word Mail Merge Vulnerability"" (CVE-2000-0788)."  
  
[CVE-2002-0693] Buffer overflow in the HTML Help ActiveX Control (hhctrl.ocx) in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows remote attackers to execute code via (1) a long parameter to the Alink function, or (2) script containing a long argument to the showHelp function.  
  
[CVE-2002-0694] "The HTML Help facility in Microsoft Windows 98, 98 Second Edition, Millennium Edition, NT 4.0, NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP uses the Local Computer Security Zone when opening .chm files from the Temporary Internet Files folder, which allows remote attackers to execute arbitrary code via HTML mail that references or inserts a malicious .chm file containing shortcuts that can be executed, aka ""Code Execution via Compiled HTML Help File."""  
  
[CVE-2002-0699] Unknown vulnerability in the Certificate Enrollment ActiveX Control in Microsoft Windows 98, Windows 98 Second Edition, Windows Millennium, Windows NT 4.0, Windows 2000, and Windows XP allow remote attackers to delete digital certificates on a user's system via HTML.  
  
[CVE-2002-0724] "Buffer overflow in SMB (Server Message Block) protocol in Microsoft Windows NT, Windows 2000, and Windows XP allows attackers to cause a denial of service (crash) via a SMB\_COM\_TRANSACTION packet with a request for the (1) NetShareEnum, (2) NetServerEnum2, or (3) NetServerEnum3, aka ""Unchecked Buffer in Network Share Provider Can Lead to Denial of Service""."  
  
[CVE-2002-0862] The (1) CertGetCertificateChain, (2) CertVerifyCertificateChainPolicy, and (3) WinVerifyTrust APIs within the CryptoAPI for Microsoft products including Microsoft Windows 98 through XP, Office for Mac, Internet Explorer for Mac, and Outlook Express for Mac, do not properly verify the Basic Constraints of intermediate CA-signed X.509 certificates, which allows remote attackers to spoof the certificates of trusted sites via a man-in-the-middle attack for SSL sessions, as originally reported for Internet Explorer and IIS.  
  
[CVE-2002-0863] "Remote Data Protocol (RDP) version 5.0 in Microsoft Windows 2000 and RDP 5.1 in Windows XP does not encrypt the checksums of plaintext session data, which could allow a remote attacker to determine the contents of encrypted sessions via sniffing, aka ""Weak Encryption in RDP Protocol."""  
  
[CVE-2002-0864] "The Remote Data Protocol (RDP) version 5.1 in Microsoft Windows XP allows remote attackers to cause a denial of service (crash) when Remote Desktop is enabled via a PDU Confirm Active data packet that does not set the Pattern BLT command, aka ""Denial of Service in Remote Desktop."""  
  
[CVE-2002-1139] "The Compressed Folders feature in Microsoft Windows 98 with Plus! Pack, Windows Me, and Windows XP does not properly check the destination folder during the decompression of ZIP files, which allows attackers to place an executable file in a known location on a user's system, aka ""Incorrect Target Path for Zipped File Decompression."""  
  
[CVE-2002-1183] "Microsoft Windows 98 and Windows NT 4.0 do not properly verify the Basic Constraints of digital certificates, allowing remote attackers to execute code, aka ""New Variant of Certificate Validation Flaw Could Enable Identity Spoofing"" (CAN-2002-0862)."  
  
[CVE-2002-1184] The system root folder of Microsoft Windows 2000 has default permissions of Everyone group with Full access (Everyone:F) and is in the search path when locating programs during login or application launch from the desktop, which could allow attackers to gain privileges as other users via Trojan horse programs.  
  
[CVE-2002-1214] Buffer overflow in Microsoft PPTP Service on Windows XP and Windows 2000 allows remote attackers to cause a denial of service (hang) and possibly execute arbitrary code via a certain PPTP packet with malformed control data.  
  
[CVE-2002-1256] The SMB signing capability in the Server Message Block (SMB) protocol in Microsoft Windows 2000 and Windows XP allows attackers to disable the digital signing settings in an SMB session to force the data to be sent unsigned, then inject data into the session without detection, e.g. by modifying group policy information sent from a domain controller.  
  
[CVE-2002-1327] "Buffer overflow in the Windows Shell function in Microsoft Windows XP allows remote attackers to execute arbitrary code via an .MP3 or .WMA audio file with a corrupt custom attribute, aka ""Unchecked Buffer in Windows Shell Could Enable System Compromise."""  
  
[CVE-2002-1561] The RPC component in Windows 2000, Windows NT 4.0, and Windows XP allows remote attackers to cause a denial of service (disabled RPC service) via a malformed packet to the RPC Endpoint Mapper at TCP port 135, which triggers a null pointer dereference.  
  
[CVE-2002-1670] Microsoft Windows XP Professional upgrade edition overwrites previously installed patches for Internet Explorer 6.0, leaving Internet Explorer unpatched.  
  
[CVE-2002-1692] Buffer overflow in backup utility of Microsoft Windows 95 allows attackers to execute arbitrary code by causing a filename with a long extension to be placed in a folder to be backed up.  
  
[CVE-2002-1712] Microsoft Windows 2000 allows remote attackers to cause a denial of service (memory consumption) by sending a flood of empty TCP/IP packets with the ACK and FIN bits set to the NetBIOS port (TCP/139), as demonstrated by stream3.  
  
[CVE-2002-1844] Microsoft Windows Media Player (WMP) 6.3, when installed on Solaris, installs executables with world-writable permissions, which allows local users to delete or modify the executables to gain privileges.  
  
[CVE-2002-1847] Buffer overflow in mplay32.exe of Microsoft Windows Media Player (WMP) 6.3 through 7.1 allows remote attackers to execute arbitrary commands via a long mp3 filename command line argument. NOTE: since the only known attack vector requires command line access, this may not be a vulnerability.  
  
[CVE-2002-1873] Microsoft Exchange 2000, when used with Microsoft Remote Procedure Call (MSRPC), allows remote attackers to cause a denial of service (crash or memory consumption) via malformed MSRPC calls.  
  
[CVE-2002-1932] "Microsoft Windows XP and Windows 2000, when configured to send administrative alerts and the ""Do not overwrite events (clear log manually)"" option is set, does not notify the administrator when the log reaches its maximum size, which allows local users and remote attackers to avoid detection."  
  
[CVE-2002-1933] The terminal services screensaver for Microsoft Windows 2000 does not automatically lock the terminal window if the window is minimized, which could allow local users to gain access to the terminal server window.  
  
[CVE-2002-1984] "Microsoft Internet Explorer 5.0.1 through 6.0 on Windows 2000 or Windows XP allows remote attackers to cause a denial of service (crash) via an OBJECT tag that contains a crafted CLASSID (CLSID) value of ""CLSID:00022613-0000-0000-C000-000000000046""."  
  
[CVE-2002-2073] Cross-site scripting (XSS) vulnerability in the default ASP pages on Microsoft Site Server 3.0 on Windows NT 4.0 allows remote attackers to inject arbitrary web script or HTML via the (1) ctr parameter in Default.asp and (2) the query string to formslogin.asp.  
  
[CVE-2002-2105] Microsoft Windows XP allows local users to prevent the system from booting via a corrupt explorer.exe.manifest file.  
  
[CVE-2002-2117] Microsoft Windows XP allows remote attackers to cause a denial of service (CPU consumption) by flooding UDP port 500 (ISAKMP).  
  
[CVE-2002-2283] "Microsoft Windows XP with Fast User Switching (FUS) enabled does not remove the ""show processes from all users"" privilege when the user is removed from the administrator group, which allows that user to view processes of other users."  
  
[CVE-2003-0004] Buffer overflow in the Windows Redirector function in Microsoft Windows XP allows local users to execute arbitrary code via a long parameter.  
  
[CVE-2003-0009] Cross-site scripting (XSS) vulnerability in Help and Support Center for Microsoft Windows Me allows remote attackers to execute arbitrary script in the Local Computer security context via an hcp:// URL with the malicious script in the topic parameter.  
  
[CVE-2003-0109] Buffer overflow in ntdll.dll on Microsoft Windows NT 4.0, Windows NT 4.0 Terminal Server Edition, Windows 2000, and Windows XP allows remote attackers to execute arbitrary code, as demonstrated via a WebDAV request to IIS 5.0.  
  
[CVE-2003-0111] "The ByteCode Verifier component of Microsoft Virtual Machine (VM) build 5.0.3809 and earlier, as used in Windows and Internet Explorer, allows remote attackers to bypass security checks and execute arbitrary code via a malicious Java applet, aka ""Flaw in Microsoft VM Could Enable System Compromise."""  
  
[CVE-2003-0227] The logging capability for unicast and multicast transmissions in the ISAPI extension for Microsoft Windows Media Services in Microsoft Windows NT 4.0 and 2000, nsiislog.dll, allows remote attackers to cause a denial of service in Internet Information Server (IIS) and execute arbitrary code via a certain network request.  
  
[CVE-2003-0228] Directory traversal vulnerability in Microsoft Windows Media Player 7.1 and Windows Media Player for Windows XP allows remote attackers to execute arbitrary code via a skins file with a URL containing hex-encoded backslash characters (%5C) that causes an executable to be placed in an arbitrary location.  
  
[CVE-2003-0345] Buffer overflow in the SMB capability for Microsoft Windows XP, 2000, and NT allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is required.  
  
[CVE-2003-0346] Multiple integer overflows in a Microsoft Windows DirectX MIDI library (QUARTZ.DLL) allow remote attackers to execute arbitrary code via a MIDI (.mid) file with (1) large length for a Text or Copyright string, or (2) a large number of tracks, which leads to a heap-based buffer overflow.  
  
[CVE-2003-0348] A certain Microsoft Windows Media Player 9 Series ActiveX control allows remote attackers to view and manipulate the Media Library on the local system via HTML script.  
  
[CVE-2003-0349] Buffer overflow in the streaming media component for logging multicast requests in the ISAPI for the logging capability of Microsoft Windows Media Services (nsiislog.dll), as installed in IIS 5.0, allows remote attackers to execute arbitrary code via a large POST request to nsiislog.dll.  
  
[CVE-2003-0496] Microsoft SQL Server before Windows 2000 SP4 allows local users to gain privileges as the SQL Server user by calling the xp\_fileexist extended stored procedure with a named pipe as an argument instead of a normal file.  
  
[CVE-2003-0533] Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPROMO.LOG log file, as exploited by the Sasser worm.  
  
[CVE-2003-0604] Windows Media Player (WMP) 7 and 8, as running on Internet Explorer and possibly other Microsoft products that process HTML, allows remote attackers to bypass zone restrictions and access or execute arbitrary files via an IFRAME tag pointing to an ASF file whose Content-location contains a File:// URL.  
  
[CVE-2003-0605] The RPC DCOM interface in Windows 2000 SP3 and SP4 allows remote attackers to cause a denial of service (crash), and local attackers to use the DoS to hijack the epmapper pipe to gain privileges, via certain messages to the \_\_RemoteGetClassObject interface that cause a NULL pointer to be passed to the PerformScmStage function.  
  
[CVE-2003-0660] The Authenticode capability in Microsoft Windows NT through Server 2003 does not prompt the user to download and install ActiveX controls when the system is low on memory, which could allow remote attackers to execute arbitrary code without user approval.  
  
[CVE-2003-0662] Buffer overflow in Troubleshooter ActiveX Control (Tshoot.ocx) in Microsoft Windows 2000 SP4 and earlier allows remote attackers to execute arbitrary code via an HTML document with a long argument to the RunQuery2 method.  
  
[CVE-2003-0719] Buffer overflow in the Private Communications Transport (PCT) protocol implementation in the Microsoft SSL library, as used in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via PCT 1.0 handshake packets.  
  
[CVE-2003-0806] Buffer overflow in the Windows logon process (winlogon) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, and XP SP1, when a member of a domain, allows remote attackers to execute arbitrary code.  
  
[CVE-2003-0812] "Stack-based buffer overflow in a logging function for Windows Workstation Service (WKSSVC.DLL) allows remote attackers to execute arbitrary code via RPC calls that cause long entries to be written to a debug log file (""NetSetup.LOG""), as demonstrated using the NetAddAlternateComputerName API."  
  
[CVE-2003-0813] A multi-threaded race condition in the Windows RPC DCOM functionality with the MS03-039 patch installed allows remote attackers to cause a denial of service (crash or reboot) by causing two threads to process the same RPC request, which causes one thread to use memory after it has been freed, a different vulnerability than CVE-2003-0352 (Blaster/Nachi), CVE-2003-0715, and CVE-2003-0528, and as demonstrated by certain exploits against those vulnerabilities.  
  
[CVE-2003-0818] Multiple integer overflows in Microsoft ASN.1 library (MSASN1.DLL), as used in LSASS.EXE, CRYPT32.DLL, and other Microsoft executables and libraries on Windows NT 4.0, 2000, and XP, allow remote attackers to execute arbitrary code via ASN.1 BER encodings with (1) very large length fields that cause arbitrary heap data to be overwritten, or (2) modified bit strings.  
  
[CVE-2003-0825] The Windows Internet Naming Service (WINS) for Microsoft Windows Server 2003, and possibly Windows NT and Server 2000, does not properly validate the length of certain packets, which allows attackers to cause a denial of service and possibly execute arbitrary code.  
  
[CVE-2003-0839] "Directory traversal vulnerability in the ""Shell Folders"" capability in Microsoft Windows Server 2003 allows remote attackers to read arbitrary files via .. (dot dot) sequences in a ""shell:"" link."  
  
[CVE-2003-0906] Buffer overflow in the rendering for (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, and XP SP1 allows remote attackers to execute arbitrary code via a malformed WMF or EMF image.  
  
[CVE-2003-0907] Help and Support Center in Microsoft Windows XP SP1 does not properly validate HCP URLs, which allows remote attackers to execute arbitrary code via quotation marks in an hcp:// URL, which are not quoted when constructing the argument list to HelpCtr.exe.  
  
[CVE-2003-0908] "The Utility Manager in Microsoft Windows 2000 executes winhlp32.exe with system privileges, which allows local users to execute arbitrary code via a ""Shatter"" style attack using a Windows message that accesses the context sensitive help button in the GUI, as demonstrated using the File Open dialog in the Help window, a different vulnerability than CVE-2004-0213."  
  
[CVE-2003-0995] Buffer overflow in the Microsoft Message Queue Manager (MSQM) allows remote attackers to cause a denial of service (RPC service crash) via a queue registration request.  
  
[CVE-2003-1106] The SMTP service in Microsoft Windows 2000 before SP4 allows remote attackers to cause a denial of service (crash or hang) via an e-mail message with a malformed time stamp in the FILETIME attribute.  
  
[CVE-2003-1107] The DHTML capability in Microsoft Windows Media Player (WMP) 6.4, 7.0, 7.1, and 9 may run certain URL commands from a security zone that is less trusted than the current zone, which allows attackers to bypass intended access restrictions.  
  
[CVE-2004-0120] The Microsoft Secure Sockets Layer (SSL) library, as used in Windows 2000, Windows XP, and Windows Server 2003, allows remote attackers to cause a denial of service via malformed SSL messages.  
  
[CVE-2004-0199] Help and Support Center in Microsoft Windows XP and Windows Server 2003 SP1 does not properly validate HCP URLs, which allows remote attackers to execute arbitrary code, as demonstrated using certain hcp:// URLs that access the DVD Upgrade capability (dvdupgrd.htm).  
  
[CVE-2004-0201] Heap-based buffer overflow in the HtmlHelp program (hh.exe) in HTML Help for Microsoft Windows 98, Me, NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary commands via a .CHM file with a large length field, a different vulnerability than CVE-2003-1041.  
  
[CVE-2004-0202] IDirectPlay4 Application Programming Interface (API) of Microsoft DirectPlay 7.0a thru 9.0b, as used in Windows Server 2003 and earlier allows remote attackers to cause a denial of service (application crash) via a malformed packet.  
  
[CVE-2004-0206] "Network Dynamic Data Exchange (NetDDE) services for Microsoft Windows 98, Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows attackers to remotely execute arbitrary code or locally gain privileges via a malicious message or application that involves an ""unchecked buffer,"" possibly a buffer overflow."  
  
[CVE-2004-0207] """Shatter"" style vulnerability in the Window Management application programming interface (API) for Microsoft Windows 98, Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows local users to gain privileges by using certain API functions to change properties of privileged programs using the SetWindowLong and SetWIndowLongPtr API functions."  
  
[CVE-2004-0208] The Virtual DOS Machine (VDM) subsystem of Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 allows local users to access kernel memory and gain privileges via a malicious program that modified some system structures in a way that is not properly validated by privileged operating system functions.  
  
[CVE-2004-0209] "Unknown vulnerability in the Graphics Rendering Engine processes of Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code via (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats that involve ""an unchecked buffer."""  
  
[CVE-2004-0210] The POSIX component of Microsoft Windows NT and Windows 2000 allows local users to execute arbitrary code via certain parameters, possibly by modifying message length values and causing a buffer overflow.  
  
[CVE-2004-0211] The kernel for Microsoft Windows Server 2003 does not reset certain values in CPU data structures, which allows local users to cause a denial of service (system crash) via a malicious program.  
  
[CVE-2004-0214] Buffer overflow in Microsoft Internet Explorer and Explorer on Windows XP SP1, WIndows 2000, Windows 98, and Windows Me may allow remote malicious servers to cause a denial of service (application crash) and possibly execute arbitrary code via long share names, as demonstrated using Samba.  
  
[CVE-2004-0503] Microsoft Outlook 2003 allows remote attackers to bypass the default zone restrictions and execute script within media files via a Rich Text Format (RTF) message containing an OLE object for the Windows Media Player, which bypasses Media Player's setting to disallow scripting and may lead to unprompted installation of an executable when exploited in conjunction with predictable-file-location exposures such as CVE-2004-0502.  
  
[CVE-2004-0540] Microsoft Windows 2000, when running in a domain whose Fully Qualified Domain Name (FQDN) is exactly 8 characters long, does not prevent users with expired passwords from logging on to the domain.  
  
[CVE-2004-0571] "Microsoft Word for Windows 6.0 Converter does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka ""Table Conversion Vulnerability,"" a different vulnerability than CVE-2004-0901."  
  
[CVE-2004-0572] Buffer overflow in the Windows Program Group Converter (grpconv.exe) may allow remote attackers to execute arbitrary code via a shell: URL with a long filename and a .grp extension, which is not properly handled when the shell capability launches grpconv.exe.  
  
[CVE-2004-0574] "The Network News Transfer Protocol (NNTP) component of Microsoft Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003, Exchange 2000 Server, and Exchange Server 2003 allows remote attackers to execute arbitrary code via XPAT patterns, possibly related to improper length validation and an ""unchecked buffer,"" leading to off-by-one and heap-based buffer overflows."  
  
[CVE-2004-0575] "Integer overflow in DUNZIP32.DLL for Microsoft Windows XP, Windows XP 64-bit Edition, Windows Server 2003, and Windows Server 2003 64-bit Edition allows remote attackers to execute arbitrary code via compressed (zipped) folders that involve an ""unchecked buffer"" and improper length validation."  
  
[CVE-2004-0726] The Windows Media Player control in Microsoft Windows 2000 allows remote attackers to execute arbitrary script in the local computer zone via an ASX filename that contains javascript, which is executed in the local context in a preview panel.  
  
[CVE-2004-0727] "Microsoft Internet Explorer 6.0.2800.1106 on Microsoft Windows XP SP2, and other versions including 5.01 and 5.5, allows remote web servers to bypass zone restrictions and execute arbitrary code in the local computer zone by redirecting a function to another function with the same name, as demonstrated by SimilarMethodNameRedir, aka the ""Similar Method Name Redirection Cross Domain Vulnerability."""  
  
[CVE-2004-0840] The SMTP (Simple Mail Transfer Protocol) component of Microsoft Windows XP 64-bit Edition, Windows Server 2003, Windows Server 2003 64-bit Edition, and the Exchange Routing Engine component of Exchange Server 2003, allows remote attackers to execute arbitrary code via a malicious DNS response message containing length values that are not properly validated.  
  
[CVE-2004-0897] The Indexing Service for Microsoft Windows XP and Server 2003 does not properly validate the length of a message, which allows remote attackers to execute arbitrary code via a buffer overflow attack.  
  
[CVE-2004-0899] "The DHCP Server service for Microsoft Windows NT 4.0 Server and Terminal Server Edition, with DHCP logging enabled, does not properly validate the length of certain messages, which allows remote attackers to cause a denial of service (application crash) via a malformed DHCP message, aka ""Logging Vulnerability."""  
  
[CVE-2004-0900] "The DHCP Server service for Microsoft Windows NT 4.0 Server and Terminal Server Edition does not properly validate the length of certain messages, which allows remote attackers to execute arbitrary code via a malformed DHCP message, aka the ""DHCP Request Vulnerability."""  
  
[CVE-2004-0901] "Microsoft Word for Windows 6.0 Converter (MSWRD632.WPC), as used in WordPad, does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka ""Font Conversion Vulnerability,"" a different vulnerability than CVE-2004-0571."  
  
[CVE-2004-1049] "Integer overflow in the LoadImage API of the USER32 Lib for Microsoft Windows allows remote attackers to execute arbitrary code via a .bmp, .cur, .ico or .ani file with a large image size field, which leads to a buffer overflow, aka the ""Cursor and Icon Format Handling Vulnerability."""  
  
[CVE-2004-1080] "The WINS service (wins.exe) on Microsoft Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 allows remote attackers to write to arbitrary memory locations and possibly execute arbitrary code via a modified memory pointer in a WINS replication packet to TCP port 42, aka the ""Association Context Vulnerability."""  
  
[CVE-2004-1324] The Microsoft Windows Media Player 9.0 ActiveX control may allow remote attackers to execute arbitrary web script in the Local computer zone via the (1) artist or (2) song fields of a music file, if the file is processed using Internet Explorer.  
  
[CVE-2004-1325] The getItemInfoByAtom function in the ActiveX control for Microsoft Windows Media Player 9.0 returns a 0 if the file does not exist and the size of the file if the file exists, which allows remote attackers to determine the existence of files on the local system.  
  
[CVE-2004-1889] Unknown vulnerability in ftpd in SGI IRIX 6.5.20 through 6.5.23 allows remote attackers to cause a denial of service (hang) via a link failure with Microsoft Windows.  
  
[CVE-2004-2176] The Internet Connection Firewall (ICF) in Microsoft Windows XP SP2 is configured by default to trust sessmgr.exe, which allows local users to use sessmgr.exe to create a local listening port that bypasses the ICF access controls.  
  
[CVE-2004-2289] Microsoft Windows XP Explorer allows local users to execute arbitrary code via a system folder with a Desktop.ini file containing a .ShellClassInfo specifier with a CLSID value that is associated with an executable file.  
  
[CVE-2004-2290] Microsoft Windows XP Explorer allows attackers to execute arbitrary code via a HTML and script in a self-executing folder that references an executable file within the folder, which is automatically executed when a user accesses the folder.  
  
[CVE-2004-2291] Microsoft Windows Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via an embedded script that uses Shell Helper objects and a shortcut (link) to execute the target script.  
  
[CVE-2004-2307] Microsoft Internet Explorer 6.0.2600 on Windows XP allows remote attackers to cause a denial of service (browser crash) via a shell: URI with double backslashes (\\) in an HTML tag such as IFRAME or A.  
  
[CVE-2004-2339] \*\* DISPUTED \*\* Microsoft Windows 2000, XP, and possibly 2003 allows local users with the SeDebugPrivilege privilege to execute arbitrary code as kernel and read or write kernel memory via the NtSystemDebugControl function, which does not verify its pointer arguments. Note: this issue has been disputed, since Administrator privileges are typically required to exploit this issue, thus privilege boundaries are not crossed.  
  
[CVE-2004-2365] Memory leak in Microsoft Windows XP and Windows Server 2003 allows local users to cause a denial of service (memory exhaustion) by repeatedly creating and deleting directories using a non-standard tool such as smbmount.  
  
[CVE-2004-2454] aMSN 0.90 for Microsoft Windows allows local users to obtain sensitive information such as hashed passwords from (1) hotlog.htm and (2) config.xml.  
  
[CVE-2004-2527] "The local and remote desktop login screens in Microsoft Windows XP before SP2 and 2003 allow remote attackers to cause a denial of service (CPU and memory consumption) by repeatedly using the WinKey+""U"" key combination, which causes multiple copies of Windows Utility Manager to be loaded more quickly than they can be closed when the copies detect that another instance is running."  
  
[CVE-2005-0048] "Microsoft Windows XP SP2 and earlier, 2000 SP3 and SP4, Server 2003, and older operating systems allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted IP packets with malformed options, aka the ""IP Validation Vulnerability."""  
  
[CVE-2005-0058] Buffer overflow in the Telephony Application Programming Interface (TAPI) for Microsoft Windows 98, Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Server 2003 allows attackers to elevate privileges or execute arbitrary code via a crafted message.  
  
[CVE-2005-0059] Buffer overflow in the Message Queuing component of Microsoft Windows 2000 and Windows XP SP1 allows remote attackers to execute arbitrary code via a crafted message.  
  
[CVE-2005-0060] Buffer overflow in the font processing component of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via a specially-designed application.  
  
[CVE-2005-0061] The kernel of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via certain access requests.  
  
[CVE-2005-0063] The document processing application used by the Windows Shell in Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code by modifying the CLSID stored in a file so that it is processed by HTML Application Host (MSHTA), as demonstrated using a Microsoft Word document.  
  
[CVE-2005-0545] Microsoft Windows XP Pro SP2 and Windows 2000 Server SP4 running Active Directory allow local users to bypass group policies that restrict access to hidden drives by using the browse feature in Office 10 applications such as Word or Excel, or using a flash drive. NOTE: this issue has been disputed in a followup post.  
  
[CVE-2005-0550] "Buffer overflow in Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to cause a denial of service (i.e., system crash) via a malformed request, aka ""Object Management Vulnerability""."  
  
[CVE-2005-0551] Stack-based buffer overflow in WINSRV.DLL in the Client Server Runtime System (CSRSS) process of Microsoft Windows 2000, Windows XP SP1 and SP2, and Windows Server 2003 allows local users to gain privileges via a specially-designed application that provides console window information with a long FaceName value.  
  
[CVE-2005-0771] VERITAS Backup Exec Server (beserver.exe) 9.0 through 10.0 for Windows allows remote unauthenticated attackers to modify the registry by calling methods to the RPC interface on TCP port 6106.  
  
[CVE-2005-0852] Microsoft Windows XP SP1 allows local users to cause a denial of service (system crash) via an empty datagram to a raw IP over IP socket (IP protocol 4), as originally demonstrated using code in Python 2.3.  
  
[CVE-2005-1205] The Telnet client for Microsoft Windows XP, Windows Server 2003, and Windows Services for UNIX allows remote attackers to read sensitive environment variables via the NEW-ENVIRON option with a SEND ENV\_USERVAR command.  
  
[CVE-2005-1206] "Buffer overflow in the Server Message Block (SMB) functionality for Microsoft Windows 2000, XP SP1 and SP2, and Server 2003 and SP1 allows remote attackers to execute arbitrary code via unknown vectors, aka the ""Server Message Block Vulnerability."""  
  
[CVE-2005-1207] Buffer overflow in the Web Client service in Microsoft Windows XP and Windows Server 2003 allows remote authenticated users to execute arbitrary code via a crafted WebDAV request containing special parameters.  
  
[CVE-2005-1208] "Integer overflow in Microsoft Windows 98, 2000, XP SP2 and earlier, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via a crafted compiled Help (.CHM) file with a large size field that triggers a heap-based buffer overflow, as demonstrated using a ""ms-its:"" URL in Internet Explorer."  
  
[CVE-2005-1218] The Microsoft Windows kernel in Microsoft Windows 2000 Server, Windows XP, and Windows Server 2003 allows remote attackers to cause a denial of service (crash) via crafted Remote Desktop Protocol (RDP) requests.  
  
[CVE-2005-1219] Buffer overflow in the Microsoft Color Management Module for Windows allows remote attackers to execute arbitrary code via an image with crafted ICC profile format tags.  
  
[CVE-2005-1792] Memory leak in Windows Management Instrumentation (WMI) service allows attackers to cause a denial of service (memory consumption and crash) by creating security contexts more quickly than they can be cleared from the RPC cache.  
  
[CVE-2005-1793] User32.DLL in Microsoft Windows 98SE, and possibly other operating systems, allows local and remote attackers to cause a denial of service (crash) via an icon (.ico) bitmap file with large width and height values.  
  
[CVE-2005-1978] "COM+ in Microsoft Windows does not properly ""create and use memory structures,"" which allows local users or remote attackers to execute arbitrary code."  
  
[CVE-2005-1979] "Distributed Transaction Controller in Microsoft Windows allows remote servers to cause a denial of service (MSDTC service exception and exit) via an ""unexpected protocol command during the reconnection request,"" which is not properly handled by the Transaction Internet Protocol (TIP) functionality."  
  
[CVE-2005-1980] "Distributed Transaction Controller in Microsoft Windows allows remote servers to cause a denial of service (MSDTC service hang) via a crafted Transaction Internet Protocol (TIP) message that causes DTC to repeatedly connect to a target IP and port number after an error occurs, aka the ""Distributed TIP Vulnerability."""  
  
[CVE-2005-1981] Unknown vulnerability in Microsoft Windows 2000 Server and Windows Server 2003 domain controllers allows remote authenticated users to cause a denial of service (system crash) via a crafted Kerberos message.  
  
[CVE-2005-1982] Unknown vulnerability in the PKINIT Protocol for Microsoft Windows 2000, Windows XP, and Windows Server 2003 could allow a local user to obtain information and spoof a server via a man-in-the-middle (MITM) attack between a client and a domain controller when PKINIT smart card authentication is being used.  
  
[CVE-2005-1983] Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm.  
  
[CVE-2005-1984] Buffer overflow in the Print Spooler service (Spoolsv.exe) for Microsoft Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code via a malicious message.  
  
[CVE-2005-1985] "The Client Service for NetWare (CSNW) on Microsoft Windows 2000 SP4, XP SP1 and Sp2, and Server 2003 SP1 and earlier, allows remote attackers to execute arbitrary code due to an ""unchecked buffer"" when processing certain crafted network messages."  
  
[CVE-2005-1987] "Buffer overflow in Collaboration Data Objects (CDO), as used in Microsoft Windows and Microsoft Exchange Server, allows remote attackers to execute arbitrary code when CDOSYS or CDOEX processes an e-mail message with a large header name, as demonstrated using the ""Content-Type"" string."  
  
[CVE-2005-2117] Web View in Windows Explorer on Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 does not properly handle certain HTML characters in preview fields, which allows remote user-assisted attackers to execute arbitrary code.  
  
[CVE-2005-2118] Windows Shell for Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote user-assisted attackers to execute arbitrary commands via a crafted shortcut (.lnk) file with long font properties that lead to a buffer overflow when the user views the file's properties using Windows Explorer, a different vulnerability than CVE-2005-2122.  
  
[CVE-2005-2120] "Stack-based buffer overflow in the Plug and Play (PnP) service (UMPNPMGR.DLL) in Microsoft Windows 2000 SP4, and XP SP1 and SP2, allows remote or local authenticated attackers to execute arbitrary code via a large number of ""\"" (backslash) characters in a registry key name, which triggers the overflow in a wsprintfW function call."  
  
[CVE-2005-2122] Windows Shell for Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to execute arbitrary commands via a shortcut (.lnk) file with long font properties that lead to a buffer overflow in the Client/Server Runtime Server Subsystem (CSRSS), a different vulnerability than CVE-2005-2118.  
  
[CVE-2005-2128] QUARTZ.DLL in Microsoft Windows Media Player 9 allows remote attackers to write a null byte to arbitrary memory via an AVI file with a crafted strn element with a modified length value.  
  
[CVE-2005-2224] aspnet\_wp.exe in Microsoft ASP.NET web services allows remote attackers to cause a denial of service (CPU consumption from infinite loop) via a crafted SOAP message to an RPC/Encoded method.  
  
[CVE-2005-2307] "netman.dll in Microsoft Windows Connections Manager Library allows local users to cause a denial of service (Network Connections Service crash) via a large integer argument to a particular function, aka ""Network Connection Manager Vulnerability."""  
  
[CVE-2005-2388] Buffer overflow in a certain USB driver, as used on Microsoft Windows, allows attackers to execute arbitrary code.  
  
[CVE-2005-2935] Unquoted Windows search path vulnerability in Microsoft AntiSpyware might allow local users to execute code via a malicious c:\program.exe file, which is run by AntiSpywareMain.exe when it attempts to execute gsasDtServ.exe. NOTE: it is not clear whether this overlaps CVE-2005-2940.  
  
[CVE-2005-2940] "Unquoted Windows search path vulnerability in Microsoft Antispyware 1.0.509 (Beta 1) might allow local users to gain privileges via a malicious ""program.exe"" file in the C: folder, involving the programs (1) GIANTAntiSpywareMain.exe, (2) gcASNotice.exe, (3) gcasServ.exe, (4) gcasSWUpdater.exe, or (5) GIANTAntiSpywareUpdater.exe. NOTE: it is not clear whether this overlaps CVE-2005-2935."  
  
[CVE-2005-3168] The SECEDIT command on Microsoft Windows 2000 before Update Rollup 1 for SP4, when using a security template to set Access Control Lists (ACLs) on folders, does not apply ACLs on folders that are listed after a long folder entry, which could result in less secure permissions than specified by the template.  
  
[CVE-2005-3169] "Microsoft Windows 2000 before Update Rollup 1 for SP4, when the ""audit directory service access"" policy is enabled, does not record a 565 event message for File Delete Child operations on an Active Directory object in the security event log, which could allow attackers to conduct unauthorized activities without detection."  
  
[CVE-2005-3170] The LDAP client on Microsoft Windows 2000 before Update Rollup 1 for SP4 accepts certificates using LDAP Secure Sockets Layer (LDAPS) even when the Certificate Authority (CA) is not trusted, which could allow attackers to trick users into believing that they are accessing a trusted site.  
  
[CVE-2005-3171] Microsoft Windows 2000 before Update Rollup 1 for SP4 records Event ID 1704 to indicate that Group Policy security settings were successfully updated, even when the processing fails such as when Ntuser.pol cannot be accessed, which could cause system administrators to believe that the system is compliant with the specified settings.  
  
[CVE-2005-3172] The WideCharToMultiByte function in Microsoft Windows 2000 before Update Rollup 1 for SP4 does not properly convert strings with Japanese composite characters in the last character, which could prevent the string from being null terminated and lead to data corruption or enable buffer overflow attacks.  
  
[CVE-2005-3173] Microsoft Windows 2000 before Update Rollup 1 for SP4 does not apply group policies if the user logs on using UPN credentials with a trailing dot, which prevents Windows 2000 from finding the correct domain controller and could allow the user to bypass intended restrictions.  
  
[CVE-2005-3174] Microsoft Windows 2000 before Update Rollup 1 for SP4 allows users to log on to the domain, even when their password has expired, if the fully qualified domain name (FQDN) is 8 characters long.  
  
[CVE-2005-3175] Microsoft Windows 2000 before Update Rollup 1 for SP4 allows a local administrator to unlock a computer even if it has been locked by a domain administrator, which allows the local administrator to access the session as the domain administrator.  
  
[CVE-2005-3176] Microsoft Windows 2000 before Update Rollup 1 for SP4 does not record the IP address of a Windows Terminal Services client in a security log event if the client connects successfully, which could make it easier for attackers to escape detection.  
  
[CVE-2005-3177] CHKDSK in Microsoft Windows 2000 before Update Rollup 1 for SP4, Windows XP, and Windows Server 2003, when running in fix mode, does not properly handle security descriptors if the master file table contains a large number of files or if the descriptors do not satisfy certain NTFS conventions, which could cause ACLs for some files to be reverted to less secure defaults, or cause security descriptors to be removed.  
  
[CVE-2005-3595] By default Microsoft Windows XP Home Edition installs with a blank password for the Administrator account, which allows remote attackers to gain control of the computer.  
  
[CVE-2005-3945] The SynAttackProtect protection in Microsoft Windows 2003 before SP1 and Windows 2000 before SP4 with Update Roll-up uses a hash of predictable data, which allows remote attackers to cause a denial of service (CPU consumption) via a flood of SYN packets that produce identical hash values, which slows down the hash table lookups.  
  
[CVE-2005-3981] \*\* DISPUTED \*\* NOTE: this issue has been disputed by third parties. Microsoft Windows XP, 2000, and 2003 allows local users to kill a writable process by using the CreateRemoteThread function with certain arguments on a process that has been opened using the OpenProcess function, possibly involving an invalid address for the start routine. NOTE: followup posts have disputed this issue, saying that if a user already has privileges to write to a process, then other functions could be called or the process could be terminated using PROCESS\_TERMINATE.  
  
[CVE-2005-4269] "mshtml.dll in Microsoft Windows XP, Server 2003, and Internet Explorer 6.0 SP1 allows attackers to cause a denial of service (access violation) by causing mshtml.dll to process button-focus events at the same time that a document is reloading, as seen in Microsoft Office InfoPath 2003 by repeatedly clicking the ""Delete"" button in a repeating section in a form. NOTE: the normal operation of InfoPath appears to involve a local user without any privilege boundaries, so this might not be a vulnerability in InfoPath. If no realistic scenarios exist for this problem in other products, then perhaps it should be excluded from CVE."  
  
[CVE-2005-4360] "The URL parser in Microsoft Internet Information Services (IIS) 5.1 on Windows XP Professional SP2 allows remote attackers to execute arbitrary code via multiple requests to "".dll"" followed by arguments such as ""~0"" through ""~9"", which causes ntdll.dll to produce a return value that is not correctly handled by IIS, as demonstrated using ""/\_vti\_bin/.dll/\*/~0"". NOTE: the consequence was originally believed to be only a denial of service (application crash and reboot)."  
  
[CVE-2005-4560] The Windows Graphical Device Interface library (GDI32.DLL) in Microsoft Windows allows remote attackers to execute arbitrary code via a Windows Metafile (WMF) format image with a crafted SETABORTPROC GDI Escape function call, related to the Windows Picture and Fax Viewer (SHIMGVW.DLL), a different vulnerability than CVE-2005-2123 and CVE-2005-2124, and as originally discovered in the wild on unionseek.com.  
  
[CVE-2005-4717] Microsoft Internet Explorer 6.0 on Windows NT 4.0 SP6a, Windows 2000 SP4, Windows XP SP1, Windows XP SP2, and Windows Server 2003 SP1 allows remote attackers to cause a denial of service (client crash) via a certain combination of a malformed HTML file and a CSS file that triggers a null dereference, probably related to rendering of a DIV element that contains a malformed IMG tag, as demonstrated by IEcrash.htm and IEcrash.rar.  
  
[CVE-2006-0005] Buffer overflow in the plug-in for Microsoft Windows Media Player (WMP) 9 and 10, when used in browsers other than Internet Explorer and set as the default application to handle media files, allows remote attackers to execute arbitrary code via HTML with an EMBED element containing a long src attribute.  
  
[CVE-2006-0006] Heap-based buffer overflow in the bitmap processing routine in Microsoft Windows Media Player 7.1 on Windows 2000 SP4, Media Player 9 on Windows 2000 SP4 and XP SP1, and Media Player 10 on XP SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted bitmap (.BMP) file that specifies a size of 0 but contains additional data.  
  
[CVE-2006-0008] "The ShellAbout API call in Korean Input Method Editor (IME) in Korean versions of Microsoft Windows XP SP1 and SP2, Windows Server 2003 up to SP1, and Office 2003, allows local users to gain privileges by launching the ""shell about dialog box"" and clicking the ""End-User License Agreement"" link, which executes Notepad with the privileges of the program that displays the about box."  
  
[CVE-2006-0010] Heap-based buffer overflow in T2EMBED.DLL in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to SP1, Windows 98, and Windows ME allows remote attackers to execute arbitrary code via an e-mail message or web page with a crafted Embedded Open Type (EOT) web font that triggers the overflow during decompression.  
  
[CVE-2006-0012] "Unspecified vulnerability in Windows Explorer in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via attack vectors involving COM objects and ""crafted files and directories,"" aka the ""Windows Shell Vulnerability."""  
  
[CVE-2006-0014] "Buffer overflow in Microsoft Outlook Express 5.5 and 6 allows remote attackers to execute arbitrary code via a crafted Windows Address Book (WAB) file containing ""certain Unicode strings"" and modified length values."  
  
[CVE-2006-0020] "An unspecified Microsoft WMF parsing application, as used in Internet Explorer 5.01 SP4 on Windows 2000 SP4, and 5.5 SP2 on Windows Millennium, and possibly other versions, allows attackers to cause a denial of service (crash) and possibly execute code via a crafted WMF file with a manipulated WMF header size, possibly involving an integer overflow, a different vulnerability than CVE-2005-4560, and aka ""WMF Image Parsing Memory Corruption Vulnerability."""  
  
[CVE-2006-0021] "Microsoft Windows XP SP1 and SP2, and Server 2003 up to SP1, allows remote attackers to cause a denial of service (hang) via an IGMP packet with an invalid IP option, aka the ""IGMP v3 DoS Vulnerability."""  
  
[CVE-2006-0023] "Microsoft Windows XP SP1 and SP2 before August 2004, and possibly other operating systems and versions, uses insecure default ACLs that allow the Authenticated Users group to gain privileges by modifying critical configuration information for the (1) Simple Service Discovery Protocol (SSDP), (2) Universal Plug and Play Device Host (UPnP), (3) NetBT, (4) SCardSvr, (5) DHCP, and (6) DnsCache services, aka ""Permissive Windows Services DACLs."" NOTE: the NetBT, SCardSvr, DHCP, DnsCache already require privileged access to exploit."  
  
[CVE-2006-0025] Stack-based buffer overflow in Microsoft Windows Media Player 9 and 10 allows remote attackers to execute arbitrary code via a PNG image with a large chunk size.  
  
[CVE-2006-0032] Cross-site scripting (XSS) vulnerability in the Indexing Service in Microsoft Windows 2000, XP, and Server 2003, when the Encoding option is set to Auto Select, allows remote attackers to inject arbitrary web script or HTML via a UTF-7 encoded URL, which is injected into an error message whose charset is set to UTF-7.  
  
[CVE-2006-0143] Microsoft Windows Graphics Rendering Engine (GRE) allows remote attackers to corrupt memory and cause a denial of service (crash) via a WMF file containing (1) ExtCreateRegion or (2) ExtEscape function calls with arguments with inconsistent lengths.  
  
[CVE-2006-0561] Cisco Secure Access Control Server (ACS) 3.x for Windows stores ACS administrator passwords and the master key in the registry with insecure permissions, which allows local users and remote administrators to decrypt the passwords by using Microsoft's cryptographic API functions to obtain the plaintext version of the master key.  
  
[CVE-2006-0753] Memory leak in Microsoft Internet Explorer 6 for Windows XP Service Pack 2 allows remote attackers to cause a denial of service (memory consumption) via JavaScript that uses setInterval to repeatedly call a function to set the value of window.status.  
  
[CVE-2006-0988] The default configuration of the DNS Server service on Windows Server 2003 and Windows 2000, and the Microsoft DNS Server service on Windows NT 4.0, allows recursive queries and provides additional delegation information to arbitrary IP addresses, which allows remote attackers to cause a denial of service (traffic amplification) via DNS queries with spoofed source IP addresses.  
  
[CVE-2006-1184] Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0, 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to cause a denial of service (crash) via a BuildContextW request with a large (1) UuidString or (2) GuidIn of a certain length, which causes an out-of-range memory access, aka the MSDTC Denial of Service Vulnerability. NOTE: this is a variant of CVE-2005-2119.  
  
[CVE-2006-1300] "Microsoft .NET framework 2.0 (ASP.NET) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to bypass access restrictions via unspecified ""URL paths"" that can access Application Folder objects ""explicitly by name."""  
  
[CVE-2006-1311] "The RichEdit component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1  
[CVE-2006-1313] "Microsoft JScript 5.1, 5.5, and 5.6 on Windows 2000 SP4, and 5.6 on Windows XP, Server 2003, Windows 98 and Windows Me, will ""release objects early"" in certain cases, which results in memory corruption and allows remote attackers to execute arbitrary code."  
  
[CVE-2006-1314] Heap-based buffer overflow in the Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to execute arbitrary code via crafted first-class Mailslot messages that triggers memory corruption and bypasses size restrictions on second-class Mailslot messages.  
  
[CVE-2006-1315] "The Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka ""SMB Information Disclosure Vulnerability."""  
  
[CVE-2006-1475] Windows Firewall in Microsoft Windows XP SP2 does not produce application alerts when an application is executed using the NTFS Alternate Data Streams (ADS) filename:stream syntax, which might allow local users to launch a Trojan horse attack in which the victim does not obtain the alert that Windows Firewall would have produced for a non-ADS file.  
  
[CVE-2006-1476] "Windows Firewall in Microsoft Windows XP SP2 produces incorrect application block alerts when the application filename is "".exe"" (with no characters before the "".""), which might allow local user-assisted users to trick a user into unblocking a Trojan horse program, as demonstrated by a malicious "".exe"" program in a folder named ""Internet Explorer,"" which triggers a question about whether to unblock the ""Internet Explorer"" program."  
  
[CVE-2006-1510] Buffer overflow in calloc.c in the Microsoft Windows XP SP2 ntdll.dll system library, when used by the ILDASM disassembler in the Microsoft .NET 1.0 and 1.1 SDK, might allow user-assisted attackers to execute arbitrary code via a crafted .dll file with a large static method.  
  
[CVE-2006-1591] Heap-based buffer overflow in Microsoft Windows Help winhlp32.exe allows user-assisted attackers to execute arbitrary code via crafted embedded image data in a .hlp file.  
  
[CVE-2006-1651] "\*\* DISPUTED \*\* Microsoft ISA Server 2004 allows remote attackers to bypass certain filtering rules, including ones for (1) ICMP and (2) TCP, via IPv6 packets. NOTE: An established researcher has disputed this issue, saying that ""Neither ISA Server 2004 nor Windows 2003 Basic Firewall support IPv6 filtering ... This is different network protocol."""  
  
[CVE-2006-1654] Directory traversal vulnerability in the HP Color LaserJet 2500 Toolbox and Color LaserJet 4600 Toolbox on Microsoft Windows before 20060402 allows remote attackers to read arbitrary files via a .. (dot dot) in an HTTP GET request to TCP port 5225.  
  
[CVE-2006-2056] "Argument injection vulnerability in Internet Explorer 6 for Windows XP SP2 allows user-assisted remote attackers to modify command line arguments to an invoked mail client via "" (double quote) characters in a mailto: scheme handler, as demonstrated by launching Microsoft Outlook with an arbitrary filename as an attachment. NOTE: it is not clear whether this issue is implementation-specific or a problem in the Microsoft API."  
  
[CVE-2006-2094] "Microsoft Internet Explorer before Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1, when Prompt is configured in Security Settings, uses modal dialogs to verify that a user wishes to run an ActiveX control or perform other risky actions, which allows user-assisted remote attackers to construct a race condition that tricks a user into clicking an object or pressing keys that are actually applied to a ""Yes"" approval for executing the control."  
  
[CVE-2006-2218] "Unspecified vulnerability in Internet Explorer 6.0 on Microsoft Windows XP SP2 allows remote attackers to execute arbitrary code via ""exceptional conditions"" that trigger memory corruption, as demonstrated using an exception handler and nested object tags, a variant of CVE-2006-1992."  
  
[CVE-2006-2334] The RtlDosPathNameToNtPathName\_U API function in NTDLL.DLL in Microsoft Windows 2000 SP4 and XP SP2 does not properly convert DOS style paths with trailing spaces into NT style paths, which allows context-dependent attackers to create files that cannot be accessed through the expected DOS path or prevent access to other similarly named files in the same directory, which prevents those files from being detected or disinfected by certain anti-virus and anti-spyware software.  
  
[CVE-2006-2372] Buffer overflow in the DHCP Client service for Microsoft Windows 2000 SP4, Windows XP SP1 and SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via a crafted DHCP response.  
  
[CVE-2006-2373] "The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to execute arbitrary code by calling the MrxSmbCscIoctlOpenForCopyChunk function with the METHOD\_NEITHER method flag and an arbitrary address, possibly for kernel memory, aka the ""SMB Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2006-2374] "The Server Message Block (SMB) driver (MRXSMB.SYS) in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows local users to cause a denial of service (hang) by calling the MrxSmbCscIoctlCloseForCopyChunk with the file handle of the shadow device, which results in a deadlock, aka the ""SMB Invalid Handle Vulnerability."""  
  
[CVE-2006-2376] Integer overflow in the PolyPolygon function in Graphics Rendering Engine on Microsoft Windows 98 and Me allows remote attackers to execute arbitrary code via a Windows Metafile (WMF) or EMF image with a sum of entries in the vertext counts array and number of polygons that triggers a heap-based buffer overflow.  
  
[CVE-2006-2378] Buffer overflow in the ART Image Rendering component (jgdw400.dll) in Microsoft Windows XP SP1 and Sp2, Server 2003 SP1 and earlier, and Windows 98 and Me allows remote attackers to execute arbitrary code via a crafted ART image that causes heap corruption.  
  
[CVE-2006-2379] Buffer overflow in the TCP/IP Protocol driver in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via unknown vectors related to IP source routing.  
  
[CVE-2006-2386] Unspecified vulnerability in Microsoft Outlook Express 6 and earlier allows remote attackers to execute arbitrary code via a crafted contact record in a Windows Address Book (WAB) file.  
  
[CVE-2006-2766] Buffer overflow in INETCOMM.DLL, as used in Microsoft Internet Explorer 6.0 through 6.0 SP2, Windows Explorer, Outlook Express 6, and possibly other programs, allows remote user-assisted attackers to cause a denial of service (application crash) via a long mhtml URI in the URL value in a URL file.  
  
[CVE-2006-3209] \*\* DISPUTED \*\* The Task scheduler (at.exe) on Microsoft Windows XP spawns each scheduled process with SYSTEM permissions, which allows local users to gain privileges. NOTE: this issue has been disputed by third parties, who state that the Task scheduler is limited to the Administrators group by default upon installation.  
  
[CVE-2006-3440] "Buffer overflow in the Winsock API in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via unknown vectors, aka ""Winsock Hostname Vulnerability."""  
  
[CVE-2006-3441] Buffer overflow in the DNS Client service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted record response. NOTE: while MS06-041 implies that there is a single issue, there are multiple vectors, and likely multiple vulnerabilities, related to (1) a heap-based buffer overflow in a DNS server response to the client, (2) a DNS server response with malformed ATMA records, and (3) a length miscalculation in TXT, HINFO, X25, and ISDN records.  
  
[CVE-2006-3442] Unspecified vulnerability in Pragmatic General Multicast (PGM) in Microsoft Windows XP SP2 and earlier allows remote attackers to execute arbitrary code via a crafted multicast message.  
  
[CVE-2006-3443] "Untrusted search path vulnerability in Winlogon in Microsoft Windows 2000 SP4, when SafeDllSearchMode is disabled, allows local users to gain privileges via a malicious DLL in the UserProfile directory, aka ""User Profile Elevation of Privilege Vulnerability."""  
  
[CVE-2006-3444] "Unspecified vulnerability in the kernel in Microsoft Windows 2000 SP4, probably a buffer overflow, allows local users to obtain privileges via unspecified vectors involving an ""unchecked buffer."""  
  
[CVE-2006-3445] Integer overflow in the ReadWideString function in agentdpv.dll in Microsoft Agent on Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via a large length value in an .ACF file, which results in a heap-based buffer overflow.  
  
[CVE-2006-3448] Buffer overflow in the Step-by-Step Interactive Training in Microsoft Windows 2000 SP4, XP SP2 and Professional, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a long Syllabus string in crafted bookmark link files (cbo, cbl, or .cbm), a different issue than CVE-2005-1212.  
  
[CVE-2006-3471] Microsoft Internet Explorer 6 on Windows XP allows remote attackers to cause a denial of service (crash) via a table with a frameset as a child, which triggers a null dereference, as demonstrated using the appendChild method.  
  
[CVE-2006-3510] The Remote Data Service Object (RDS.DataControl) in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (crash) via a series of operations that result in an invalid length calculation when using SysAllocStringLen, then triggers a buffer over-read.  
  
[CVE-2006-3643] "Cross-site scripting (XSS) vulnerability in Internet Explorer 5.01 and 6 in Microsoft Windows 2000 SP4 permits access to local ""HTML-embedded resource files"" in the Microsoft Management Console (MMC) library, which allows remote authenticated users to execute arbitrary commands, aka ""MMC Redirect Cross-Site Scripting Vulnerability."""  
  
[CVE-2006-3648] "Unspecified vulnerability in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 and 2003 SP1, allows remote attackers to execute arbitrary code via unspecified vectors involving unhandled exceptions, memory resident applications, and incorrectly ""unloading chained exception."""  
  
[CVE-2006-3730] Integer overflow in Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a 0x7fffffff argument to the setSlice method on a WebViewFolderIcon ActiveX object, which leads to an invalid memory copy.  
  
[CVE-2006-3869] Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060824, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL on a website that uses HTTP 1.1 compression.  
  
[CVE-2006-3873] Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060912, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL in a GZIP-encoded website that was the target of an HTTP redirect, due to an incomplete fix for CVE-2006-3869.  
  
[CVE-2006-3880] "\*\* DISPUTED \*\* Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Small Business Server 2003 allow remote attackers to cause a denial of service (IP stack hang) via a continuous stream of packets on TCP port 135 that have incorrect TCP header checksums and random numbers in certain TCP header fields, as demonstrated by the Achilles Windows Attack Tool. NOTE: the researcher reports that the Microsoft Security Response Center has stated ""Our investigation which has included code review, review of the TCPDump, and attempts on reproing the issue on multiple fresh installs of various Windows Operating Systems have all resulted in non confirmation."""  
  
[CVE-2006-3897] Stack overflow in Microsoft Internet Explorer 6 on Windows 2000 allows remote attackers to cause a denial of service (application crash) by creating an NMSA.ASFSourceMediaDescription.1 ActiveX object with a long dispValue property.  
  
[CVE-2006-3898] Microsoft Internet Explorer 6.0 on Windows XP SP2 allows remote attackers to cause a denial of service (application crash) by calling the Click method of the Internet.HHCtrl.1 ActiveX object before initializing the URL, which triggers a null dereference.  
  
[CVE-2006-3899] Microsoft Internet Explorer 6.0 on Windows XP SP2 allows remote attackers to cause a denial of service (application crash) by calling the stringToBinary function of the CEnroll.CEnroll.2 ActiveX object with a long second argument, which triggers an invalid memory access inside the SysAllocStringLen function.  
  
[CVE-2006-3915] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by iterating over any native function, as demonstrated with the window.alert function, which triggers a null dereference.  
  
[CVE-2006-3942] "The server driver (srv.sys) in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to cause a denial of service (system crash) via an SMB\_COM\_TRANSACTION SMB message that contains a string without null character termination, which leads to a NULL dereference in the ExecuteTransaction function, possibly related to an ""SMB PIPE,"" aka the ""Mailslot DOS"" vulnerability. NOTE: the name ""Mailslot DOS"" was derived from incomplete initial research  
[CVE-2006-3943] Stack-based buffer overflow in NDFXArtEffects in Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) via long (1) RGBExtraColor, (2) RGBForeColor, and (3) RGBBackColor properties.  
  
[CVE-2006-3944] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) via a (1) Forms.ListBox.1 or (2) Forms.ListBox.1 object with the ListWidth property set to (a) 0x7fffffff, which triggers an integer overflow exception, or to (b) 0x7ffffffe, which triggers a null dereference.  
  
[CVE-2006-3992] Unspecified vulnerability in the Centrino (1) w22n50.sys, (2) w22n51.sys, (3) w29n50.sys, and (4) w29n51.sys Microsoft Windows drivers for Intel 2200BG and 2915ABG PRO/Wireless Network Connection before 10.5 with driver 9.0.4.16 allows remote attackers to execute arbitrary code via certain frames that trigger memory corruption.  
  
[CVE-2006-4066] The Graphical Device Interface Plus library (gdiplus.dll) in Microsoft Windows XP SP2 allows context-dependent attackers to cause a denial of service (application crash) via certain images that trigger a divide-by-zero error, as demonstrated by a (1) .ico file, (2) .png file that crashes MSN Messenger, and (3) .jpg file that crashes Internet Explorer. NOTE: another researcher has not been able to reproduce this issue.  
  
[CVE-2006-4071] Sign extension vulnerability in the createBrushIndirect function in the GDI library (gdi32.dll) in Microsoft Windows XP, Server 2003, and possibly other versions, allows user-assisted attackers to cause a denial of service (application crash) via a crafted WMF file.  
  
[CVE-2006-4128] Multiple heap-based buffer overflows in Symantec VERITAS Backup Exec for Netware Server Remote Agent for Windows Server 9.1 and 9.2 (all builds), Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1 (builds 10.1.325.6301, 10.1.326.1401, 10.1.326.2501, 10.1.326.3301, and 10.1.327.401), and Backup Exec for Windows Server and Remote Agent 9.1 (build 9.1.4691), 10.0 (builds 10.0.5484 and 10.0.5520), and 10.1 (build 10.1.5629) allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted RPC message.  
  
[CVE-2006-4138] Multiple unspecified vulnerabilities in Microsoft Windows Help File viewer (winhlp32.exe) allow user-assisted attackers to execute arbitrary code via crafted HLP files.  
  
[CVE-2006-4219] The Terminal Services COM object (tsuserex.dll) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by instantiating it as an ActiveX object in Internet Explorer 6.0 SP1 on Microsoft Windows 2003 EE SP1 CN.  
  
[CVE-2006-4495] Microsoft Internet Explorer allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code by instantiating certain Windows 2000 ActiveX COM Objects including (1) ciodm.dll, (2) myinfo.dll, (3) msdxm.ocx, and (4) creator.dll.  
  
[CVE-2006-4688] "Buffer overflow in Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to execute arbitrary code via crafted messages, aka ""Client Service for NetWare Memory Corruption Vulnerability."""  
  
[CVE-2006-4689] "Unspecified vulnerability in the driver for the Client Service for NetWare (CSNW) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 up to SP1 allows remote attackers to cause a denial of service (hang and reboot) via has unknown attack vectors, aka ""NetWare Driver Denial of Service Vulnerability."""  
  
[CVE-2006-4692] "Argument injection vulnerability in the Windows Object Packager (packager.exe) in Microsoft Windows XP SP1 and SP2 and Server 2003 SP1 and earlier allows remote user-assisted attackers to execute arbitrary commands via a crafted file with a ""/"" (slash) character in the filename of the Command Line property, followed by a valid file extension, which causes the command before the slash to be executed, aka ""Object Packager Dialogue Spoofing Vulnerability."""  
  
[CVE-2006-4694] Unspecified vulnerability in PowerPoint in Microsoft Office 2000, Office XP and Office 2003 allows user-assisted attackers to execute arbitrary code via a crafted record in a PPT file, as exploited by malware such as Exploit:Win32/Controlppt.W, Exploit:Win32/Controlppt.X, and Exploit-PPT.d/Trojan.PPDropper.F. NOTE: it has been reported that the attack vector involves SlideShowWindows.View.GotoNamedShow.  
  
[CVE-2006-4696] "Unspecified vulnerability in the Server service in Microsoft Windows 2000 SP4, Server 2003 SP1 and earlier, and XP SP2 and earlier allows remote attackers to execute arbitrary code via a crafted packet, aka ""SMB Rename Vulnerability."""  
  
[CVE-2006-4702] Buffer overflow in the Windows Media Format Runtime in Microsoft Windows Media Player (WMP) 6.4 and Windows XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted Advanced Systems Format (ASF) file.  
  
[CVE-2006-4868] Stack-based buffer overflow in the Vector Graphics Rendering engine (vgx.dll), as used in Microsoft Outlook and Internet Explorer 6.0 on Windows XP SP2, and possibly other versions, allows remote attackers to execute arbitrary code via a Vector Markup Language (VML) file with a long fill parameter within a rect tag.  
  
[CVE-2006-5028] Directory traversal vulnerability in filemanager/filemanager.php in SWsoft Plesk 7.5 Reload and Plesk 7.6 for Microsoft Windows allows remote attackers to list arbitrary directories via a ../ (dot dot slash) in the file parameter in a chdir action.  
  
[CVE-2006-5270] Integer overflow in the Microsoft Malware Protection Engine (mpengine.dll), as used by Windows Live OneCare, Antigen, Defender, and Forefront Security, allows user-assisted remote attackers to execute arbitrary code via a crafted PDF file.  
  
[CVE-2006-5448] "The drmstor.dll ActiveX object in Microsoft Windows Digital Rights Management System (DRM) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long parameter to the StoreLicense function, which triggers ""memory corruption"" and possibly a buffer overflow."  
  
[CVE-2006-5583] "Buffer overflow in the SNMP Service in Microsoft Windows 2000 SP4, XP SP2, Server 2003, Server 2003 SP1, and possibly other versions allows remote attackers to execute arbitrary code via a crafted SNMP packet, aka ""SNMP Memory Corruption Vulnerability."""  
  
[CVE-2006-5584] The Remote Installation Service (RIS) in Microsoft Windows 2000 SP4 uses a TFTP server that allows anonymous access, which allows remote attackers to upload and overwrite arbitrary files to gain privileges on systems that use RIS.  
  
[CVE-2006-5585] "The Client-Server Run-time Subsystem in Microsoft Windows XP SP2 and Server 2003 allows local users to gain privileges via a crafted file manifest within an application, aka ""File Manifest Corruption Vulnerability."""  
  
[CVE-2006-5586] "The Graphics Rendering Engine in Microsoft Windows 2000 SP4 and XP SP2 allows local users to gain privileges via ""invalid application window sizes"" in layered application windows, aka the ""GDI Invalid Window Size Elevation of Privilege Vulnerability."""  
  
[CVE-2006-5614] Microsoft Windows NAT Helper Components (ipnathlp.dll) on Windows XP SP2, when Internet Connection Sharing is enabled, allows remote attackers to cause a denial of service (svchost.exe crash) via a malformed DNS query, which results in a null pointer dereference.  
  
[CVE-2006-5745] Unspecified vulnerability in the setRequestHeader method in the XMLHTTP (XML HTTP) ActiveX Control 4.0 in Microsoft XML Core Services 4.0 on Windows, when accessed by Internet Explorer, allows remote attackers to execute arbitrary code via crafted arguments that lead to memory corruption, a different vulnerability than CVE-2006-4685. NOTE: some of these details are obtained from third party information.  
  
[CVE-2006-5758] The Graphics Rendering Engine in Microsoft Windows 2000 through 2000 SP4 and Windows XP through SP2 maps GDI Kernel structures on a global shared memory section that is mapped with read-only permissions, but can be remapped by other processes as read-write, which allows local users to cause a denial of service (memory corruption and crash) and gain privileges by modifying the kernel structures.  
  
[CVE-2006-6134] Heap-based buffer overflow in the WMCheckURLScheme function in WMVCORE.DLL in Microsoft Windows Media Player (WMP) 10.00.00.4036 on Windows XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to cause a denial of service (application crash) and execute arbitrary code via a long HREF attribute, using an unrecognized protocol, in a REF element in an ASX PlayList file.  
  
[CVE-2006-6252] "Microsoft Windows Live Messenger 8.0 and earlier, when gestual emoticons are enabled, allows remote attackers to cause a denial of service (CPU consumption) via a long string composed of "":D"" sequences, which are interpreted as emoticons."  
  
[CVE-2006-6579] Microsoft Windows XP has weak permissions (FILE\_WRITE\_DATA and FILE\_READ\_DATA for Everyone) for %WINDIR%\pchealth\ERRORREP\QHEADLES, which allows local users to write and read files in this folder, as demonstrated by an ASP shell that has write access by IWAM\_machine and read access by IUSR\_Machine.  
  
[CVE-2006-6601] Windows Media Player 10.00.00.4036 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service via a .MID (MIDI) file with a malformed header chunk without any track chunks, possibly involving (1) number of tracks of (2) time division fields that are set to 0.  
  
[CVE-2006-6602] explorer.exe in Windows Explorer 6.00.2900.2180 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service via a crafted WMV file.  
  
[CVE-2006-6659] The Microsoft Office Outlook Recipient ActiveX control (ole32.dll) in Windows XP SP2 allows remote attackers to cause a denial of service (Internet Explorer 7 hang) via crafted HTML.  
  
[CVE-2006-6696] Double free vulnerability in Microsoft Windows 2000, XP, 2003, and Vista allows local users to gain privileges by calling the MessageBox function with a MB\_SERVICE\_NOTIFICATION message with crafted data, which sends a HardError message to Client/Server Runtime Server Subsystem (CSRSS) process, which is not properly handled when invoking the UserHardError and GetHardErrorText functions in WINSRV.DLL.  
  
[CVE-2006-6753] Event Viewer (eventvwr.exe) in Microsoft Windows does not properly display log data that contains '%' (percent) characters, which might make it impossible to use Event Viewer to determine the actual data that triggered an event, and might produce long strings that are not properly handled by certain processes that rely on Event Viewer.  
  
[CVE-2006-6797] The Client Server Run-Time Subsystem (CSRSS) in Microsoft Windows allows local users to cause a denial of service (crash) or read arbitrary memory from csrss.exe via crafted arguments to the NtRaiseHardError function with status 0x50000018, a different vulnerability than CVE-2006-6696.  
  
[CVE-2006-6901] Unspecified vulnerability in the Bluetooth stack in Microsoft Windows allows remote attackers to gain administrative access (aka Remote Root) via unspecified vectors.  
  
[CVE-2006-6902] Unspecified vulnerability in the Bluetooth stack in Microsoft Windows Mobile Pocket PC edition allows remote attackers to gain administrative access (aka Remote Root) via unspecified vectors.  
  
[CVE-2006-7066] Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by creating an object inside an iframe, deleting the frame by setting its location.href to about:blank, then accessing a property of the object within the deleted frame, which triggers a NULL pointer dereference. NOTE: it was later reported that 7.0.6000.16473 and earlier are also affected.  
  
[CVE-2006-7206] "Microsoft Internet Explorer 6 on Windows XP SP2 allows remote attackers to cause a denial of service (crash) by creating a ADODB.Recordset object and making a series of calls to the NextRecordset method with a long string argument, which causes an ""invalid memory access"" in the SysFreeString function, a different issue than CVE-2006-3510 and CVE-2006-3899."  
  
[CVE-2006-7210] Microsoft Windows 2000, XP, and Server 2003 allows remote attackers to cause a denial of service (cpu consumption) via a PNG image with crafted (1) Width and (2) Height values in the IHDR block.  
  
[CVE-2007-0024] "Integer overflow in the Vector Markup Language (VML) implementation (vgx.dll) in Microsoft Internet Explorer 5.01, 6, and 7 on Windows 2000 SP4, XP SP2, Server 2003, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted web page that contains unspecified integer properties that cause insufficient memory allocation and trigger a buffer overflow, aka the ""VML Buffer Overrun Vulnerability."""  
  
[CVE-2007-0025] The MFC component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 and Visual Studio .NET 2000, 2002 SP1, 2003, and 2003 SP1 allows user-assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption. NOTE: this might be due to a stack-based buffer overflow in the AfxOleSetEditMenu function in MFC42u.dll.  
  
[CVE-2007-0026] The OLE Dialog component in Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 allows user-assisted remote attackers to execute arbitrary code via an RTF file with a malformed OLE object that triggers memory corruption.  
  
[CVE-2007-0038] "Stack-based buffer overflow in the animated cursor code in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a large length value in the second (or later) anih block of a RIFF .ANI, cur, or .ico file, which results in memory corruption when processing cursors, animated cursors, and icons, a variant of CVE-2005-0416, as originally demonstrated using Internet Explorer 6 and 7. NOTE: this might be a duplicate of CVE-2007-1765  
[CVE-2007-0040] "The LDAP service in Windows Active Directory in Microsoft Windows 2000 Server SP4, Server 2003 SP1 and SP2, Server 2003 x64 Edition and SP2, and Server 2003 for Itanium-based Systems SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted LDAP request with an unspecified number of ""convertible attributes."""  
  
[CVE-2007-0041] "The PE Loader service in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows remote attackers to execute arbitrary code via unspecified vectors involving an ""unchecked buffer"" and unvalidated message lengths, probably a buffer overflow."  
  
[CVE-2007-0042] "Interpretation conflict in ASP.NET in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows remote attackers to access configuration files and obtain sensitive information, and possibly bypass security mechanisms that try to constrain the final substring of a string, via %00 characters, related to use of %00 as a string terminator within POSIX functions but a data character within .NET strings, aka ""Null Byte Termination Vulnerability."""  
  
[CVE-2007-0043] "The Just In Time (JIT) Compiler service in Microsoft .NET Framework 1.0, 1.1, and 2.0 for Windows 2000, XP, Server 2003, and Vista allows user-assisted remote attackers to execute arbitrary code via unspecified vectors involving an ""unchecked buffer,"" probably a buffer overflow, aka "".NET JIT Compiler Vulnerability""."  
  
[CVE-2007-0045] "Multiple cross-site scripting (XSS) vulnerabilities in Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distributed with Adobe Reader 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2, for Mozilla Firefox, Microsoft Internet Explorer 6 SP1, Google Chrome, Opera 8.5.4 build 770, and Opera 9.10.8679 on Windows allow remote attackers to inject arbitrary JavaScript and conduct other attacks via a .pdf URL with a javascript: or res: URI with (1) FDF, (2) XML, and (3) XFDF AJAX parameters, or (4) an arbitrarily named name=URI anchor identifier, aka ""Universal XSS (UXSS)."""  
  
[CVE-2007-0064] Heap-based buffer overflow in Windows Media Format Runtime 7.1, 9, 9.5, 9.5 x64 Edition, 11, and Windows Media Services 9.1 for Microsoft Windows 2000, XP, Server 2003, and Vista allows user-assisted remote attackers to execute arbitrary code via a crafted Advanced Systems Format (ASF) file.  
  
[CVE-2007-0065] Heap-based buffer overflow in Object Linking and Embedding (OLE) Automation in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, Office 2004 for Mac, and Visual basic 6.0 SP6 allows remote attackers to execute arbitrary code via a crafted script request.  
  
[CVE-2007-0066] "The kernel in Microsoft Windows 2000 SP4, XP SP2, and Server 2003, when ICMP Router Discovery Protocol (RDP) is enabled, allows remote attackers to cause a denial of service via fragmented router advertisement ICMP packets that trigger an out-of-bounds read, aka ""Windows Kernel TCP/IP/ICMP Vulnerability."""  
  
[CVE-2007-0069] "Unspecified vulnerability in the kernel in Microsoft Windows XP SP2, Server 2003, and Vista allows remote attackers to cause a denial of service (CPU consumption) and possibly execute arbitrary code via crafted (1) IGMPv3 and (2) MLDv2 packets that trigger memory corruption, aka ""Windows Kernel TCP/IP/IGMPv3 and MLDv2 Vulnerability."""  
  
[CVE-2007-0084] \*\* DISPUTED \*\* Buffer overflow in the Windows NT Message Compiler (MC) 1.00.5239 on Microsoft Windows XP allows local users to gain privileges via a long MC-filename. NOTE: this issue has been disputed by a reliable third party who states that the compiler is not a privileged program, so privilege boundaries cannot be crossed.  
  
[CVE-2007-0210] "The Window Image Acquisition (WIA) Service in Microsoft Windows XP SP2 allows local users to gain privileges via unspecified vectors involving an ""unchecked buffer,"" probably a buffer overflow."  
  
[CVE-2007-0211] "The hardware detection functionality in the Windows Shell in Microsoft Windows XP SP2 and Professional, and Server 2003 SP1 allows local users to gain privileges via an unvalidated parameter to a function related to the ""detection and registration of new hardware."""  
  
[CVE-2007-0214] The HTML Help ActiveX control (Hhctrl.ocx) in Microsoft Windows 2000 SP3, XP SP2 and Professional, 2003 SP1 allows remote attackers to execute arbitrary code via unspecified functions, related to uninitialized parameters.  
  
[CVE-2007-0351] Microsoft Windows XP and Windows Server 2003 do not properly handle user logoff, which might allow local users to gain the privileges of a previous system user, possibly related to user profile unload failure. NOTE: it is not clear whether this is an issue in Windows itself, or an interaction with another product. The issue might involve ZoneAlarm not being able to terminate processes when it cannot prompt the user.  
  
[CVE-2007-0562] Windows Explorer (explorer.exe) 6.0.2900.2180 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted .avi file, which triggers the crash when the user right clicks on the file.  
  
[CVE-2007-0612] "Multiple ActiveX controls in Microsoft Windows 2000, XP, 2003, and Vista allows remote attackers to cause a denial of service (Internet Explorer crash) by accessing the bgColor, fgColor, linkColor, alinkColor, vlinkColor, or defaultCharset properties in the (1) giffile, (2) htmlfile, (3) jpegfile, (4) mhtmlfile, (5) ODCfile, (6) pjpegfile, (7) pngfile, (8) xbmfile, (9) xmlfile, (10) xslfile, or (11) wdfile objects in (a) mshtml.dll  
[CVE-2007-0675] A certain ActiveX control in sapi.dll (aka the Speech API) in Speech Components in Microsoft Windows Vista, when the Speech Recognition feature is enabled, allows user-assisted remote attackers to delete arbitrary files, and conduct other unauthorized activities, via a web page with an embedded sound object that contains voice commands to an enabled microphone, allowing for interaction with Windows Explorer.  
  
[CVE-2007-0811] Microsoft Internet Explorer 6.0 SP1 on Windows 2000, and 6.0 SP2 on Windows XP, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an HTML document containing a certain JavaScript for loop with an empty loop body, possibly involving getElementById.  
  
[CVE-2007-0843] The ReadDirectoryChangesW API function on Microsoft Windows 2000, XP, Server 2003, and Vista does not check permissions for child objects, which allows local users to bypass permissions by opening a directory with LIST (READ) access and using ReadDirectoryChangesW to monitor changes of files that do not have LIST permissions, which can be leveraged to determine filenames, access times, and other sensitive information.  
  
[CVE-2007-0878] "Unspecified vulnerability in Microsoft Internet Explorer on Windows Mobile 5.0 allows remote attackers to cause a denial of service (loss of browser and other device functionality) via a malformed WML page, related to an ""overflow state."" NOTE: it is possible that this issue is related to CVE-2007-0685."  
  
[CVE-2007-0942] "Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-0944] "Unspecified vulnerability in the CTableCol::OnPropertyChange method in Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-0945] "Microsoft Internet Explorer 6 SP1 on Windows 2000 SP4  
[CVE-2007-0946] "Unspecified vulnerability in Microsoft Internet Explorer 7 on Windows XP SP2, Windows Server 2003 SP1 or SP2, or Windows Vista allows remote attackers to execute arbitrary code via crafted HTML objects, which results in memory corruption, aka the first of two ""HTML Objects Memory Corruption Vulnerabilities"" and a different issue than CVE-2007-0947."  
  
[CVE-2007-0947] "Use-after-free vulnerability in Microsoft Internet Explorer 7 on Windows XP SP2, Windows Server 2003 SP1 or SP2, or Windows Vista allows remote attackers to execute arbitrary code via crafted HTML objects, resulting in accessing deallocated memory of CMarkup objects, aka the second of two ""HTML Objects Memory Corruption Vulnerabilities"" and a different issue than CVE-2007-0946."  
  
[CVE-2007-1070] Multiple stack-based buffer overflows in Trend Micro ServerProtect for Windows and EMC 5.58, and for Network Appliance Filer 5.61 and 5.62, allow remote attackers to execute arbitrary code via crafted RPC requests to TmRpcSrv.dll that trigger overflows when calling the (1) CMON\_NetTestConnection, (2) CMON\_ActiveUpdate, and (3) CMON\_ActiveRollback functions in (a) StCommon.dll, and (4) ENG\_SetRealTimeScanConfigInfo and (5) ENG\_SendEMail functions in (b) eng50.dll.  
  
[CVE-2007-1090] Microsoft Windows Explorer on Windows XP and 2003 allows remote user-assisted attackers to cause a denial of service (crash) via a malformed WMF file, which triggers the crash when the user browses the folder.  
  
[CVE-2007-1204] Stack-based buffer overflow in the Universal Plug and Play (UPnP) service in Microsoft Windows XP SP2 allows remote attackers on the same subnet to execute arbitrary code via crafted HTTP headers in request or notification messages, which trigger memory corruption.  
  
[CVE-2007-1205] Unspecified vulnerability in Microsoft Agent (msagent\agentsvr.exe) in Windows 2000 SP4, XP SP2, and Server 2003, 2003 SP1, and 2003 SP2 allows remote attackers to execute arbitrary code via crafted URLs, which result in memory corruption.  
  
[CVE-2007-1206] "The Virtual DOS Machine (VDM) in the Windows Kernel in Microsoft Windows NT 4.0  
[CVE-2007-1209] "Use-after-free vulnerability in the Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Vista does not properly handle connection resources when starting and stopping processes, which allows local users to gain privileges by opening and closing multiple ApiPort connections, which leaves a ""dangling pointer"" to a process data structure."  
  
[CVE-2007-1211] "Unspecified kernel GDI functions in Microsoft Windows 2000 SP4  
[CVE-2007-1212] "Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4  
[CVE-2007-1213] The TrueType Fonts rasterizer in Microsoft Windows 2000 SP4 allows local users to gain privileges via crafted TrueType fonts, which result in an uninitialized function pointer.  
  
[CVE-2007-1215] "Buffer overflow in the Graphics Device Interface (GDI) in Microsoft Windows 2000 SP4  
[CVE-2007-1347] Microsoft Windows Explorer on Windows 2000 SP4 FR and XP SP2 FR, and possibly other versions and platforms, allows remote attackers to cause a denial of service (memory corruption and crash) via an Office file with crafted document summary information, which causes an error in Ole32.dll.  
  
[CVE-2007-1492] winmm.dll in Microsoft Windows XP allows user-assisted remote attackers to cause a denial of service (infinite loop) via a large cch argument value to the mmioRead function, as demonstrated by a crafted WAV file.  
  
[CVE-2007-1499] "Microsoft Internet Explorer 7.0 on Windows XP and Vista allows remote attackers to conduct phishing attacks and possibly execute arbitrary code via a res: URI to navcancl.htm with an arbitrary URL as an argument, which displays the URL in the location bar of the ""Navigation Canceled"" page and injects the script into the ""Refresh the page"" link, aka Navigation Cancel Page Spoofing Vulnerability."""  
  
[CVE-2007-1512] "Stack-based buffer overflow in the AfxOleSetEditMenu function in the MFC component in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 Gold and SP1, and Visual Studio .NET 2002 Gold and SP1, and 2003 Gold and SP1 allows user-assisted remote attackers to have an unknown impact (probably crash) via an RTF file with a malformed OLE object, which results in writing two 0x00 characters past the end of szBuffer, aka the ""MFC42u.dll Off-by-Two Overflow."" NOTE: this issue is due to an incomplete patch (MS07-012) for CVE-2007-0025."  
  
[CVE-2007-1527] "The LLTD Mapper in Microsoft Windows Vista does not verify that an IP address in a TLV type 0x07 field in a HELLO packet corresponds to a valid IP address for the local network, which allows remote attackers to trick users into communicating with an external host by sending a HELLO packet with the MW characteristic and a spoofed TLV type 0x07 field, aka the ""Spoof and Management URL IP Redirect"" attack."  
  
[CVE-2007-1528] "The LLTD Mapper in Microsoft Windows Vista allows remote attackers to spoof hosts, and nonexistent bridge relationships, into the network topology map by using a MAC address that differs from the MAC address provided in the Real Source field of the LLTD BASE header of a HELLO packet, aka the ""Spoof on Bridge"" attack."  
  
[CVE-2007-1529] "The LLTD Responder in Microsoft Windows Vista does not send the Mapper a response to a DISCOVERY packet if another host has sent a spoofed response first, which allows remote attackers to spoof arbitrary hosts via a network-based race condition, aka the ""Total Spoof"" attack."  
  
[CVE-2007-1530] The LLTD Mapper in Microsoft Windows Vista does not properly gather responses to EMIT packets, which allows remote attackers to cause a denial of service (mapping failure) by omitting an ACK response, which triggers an XML syntax error.  
  
[CVE-2007-1531] Microsoft Windows XP and Vista overwrites ARP table entries included in gratuitous ARP, which allows remote attackers to cause a denial of service (loss of network access) by sending a gratuitous ARP for the address of the Vista host.  
  
[CVE-2007-1532] The neighbor discovery implementation in Microsoft Windows Vista allows remote attackers to conduct a redirect attack by (1) responding to queries by sending spoofed Neighbor Advertisements or (2) blindly sending Neighbor Advertisements.  
  
[CVE-2007-1533] The Teredo implementation in Microsoft Windows Vista uses the same nonce for communication with different UDP ports within a solicitation session, which makes it easier for remote attackers to spoof the nonce through brute force attacks.  
  
[CVE-2007-1534] DFSR.exe in Windows Meeting Space in Microsoft Windows Vista remains available for remote connections on TCP port 5722 for 2 minutes after Windows Meeting Space is closed, which allows remote attackers to have an unknown impact by connecting to this port during the time window.  
  
[CVE-2007-1535] Microsoft Windows Vista establishes a Teredo address without user action upon connection to the Internet, contrary to documentation that Teredo is inactive without user action, which increases the attack surface and allows remote attackers to communicate via Teredo.  
  
[CVE-2007-1537] \Device\NdisTapi (NDISTAPI.sys) in Microsoft Windows XP SP2 and 2003 SP1 uses weak permissions, which allows local users to write to the device and cause a denial of service, as demonstrated by using an IRQL to acquire a spinlock on paged memory via the NdisTapiDispatch function.  
  
[CVE-2007-1644] The dynamic DNS update mechanism in the DNS Server service on Microsoft Windows does not properly authenticate clients in certain deployments or configurations, which allows remote attackers to change DNS records for a web proxy server and conduct man-in-the-middle (MITM) attacks on web traffic, conduct pharming attacks by poisoning DNS records, and cause a denial of service (erroneous name resolution).  
  
[CVE-2007-1645] Buffer overflow in FutureSoft TFTP Server 2000 on Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via a long request on UDP port 69. NOTE: this issue might overlap CVE-2006-4781 or CVE-2005-1812.  
  
[CVE-2007-1658] Windows Mail in Microsoft Windows Vista might allow user-assisted remote attackers to execute certain programs via a link to a (1) local file or (2) UNC share pathname in which there is a directory with the same base name as an executable program at the same level, as demonstrated using C:/windows/system32/winrm (winrm.cmd) and migwiz (migwiz.exe).  
  
[CVE-2007-1692] The default configuration of Microsoft Windows uses the Web Proxy Autodiscovery Protocol (WPAD) without static WPAD entries, which might allow remote attackers to intercept web traffic by registering a proxy server using WINS or DNS, then responding to WPAD requests, as demonstrated using Internet Explorer. NOTE: it could be argued that if an attacker already has control over WINS/DNS, then web traffic could already be intercepted by modifying WINS or DNS records, so this would not cross privilege boundaries and would not be a vulnerability. It has also been reported that DHCP is an alternate attack vector.  
  
[CVE-2007-1763] The ATI kernel driver (atikmdag.sys) in Microsoft Windows Vista allows user-assisted remote attackers to cause a denial of service (crash) via a crafted JPG image, as demonstrated by a slideshow, possibly due to a buffer overflow.  
  
[CVE-2007-1765] "Unspecified vulnerability in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a malformed ANI file, which results in memory corruption when processing cursors, animated cursors, and icons, a similar issue to CVE-2005-0416, as originally demonstrated using Internet Explorer 6 and 7. NOTE: this issue might be a duplicate of CVE-2007-0038  
[CVE-2007-1912] Heap-based buffer overflow in Microsoft Windows allows user-assisted remote attackers to have an unknown impact via a crafted .HLP file.  
  
[CVE-2007-1946] Integer overflow in Windows Explorer in Microsoft Windows XP SP1 might allow user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large width dimension in a crafted BMP image, as demonstrated by w4intof.bmp.  
  
[CVE-2007-1973] Race condition in the Virtual DOS Machine (VDM) in the Windows Kernel in Microsoft Windows NT 4.0 allows local users to modify memory and gain privileges via the temporary \Device\PhysicalMemory section handle, a related issue to CVE-2007-1206.  
  
[CVE-2007-2217] Kodak Image Viewer in Microsoft Windows 2000 SP4, and in some cases XP SP2 and Server 2003 SP1 and SP2, allows remote attackers to execute arbitrary code via crafted image files that trigger memory corruption, as demonstrated by a certain .tif (TIFF) file.  
  
[CVE-2007-2218] Unspecified vulnerability in the Windows Schannel Security Package for Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2, allows remote servers to execute arbitrary code or cause a denial of service via crafted digital signatures that are processed during an SSL handshake.  
  
[CVE-2007-2219] Unspecified vulnerability in the Win32 API on Microsoft Windows 2000, XP SP2, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via certain parameters to an unspecified function.  
  
[CVE-2007-2221] "Unspecified vulnerability in the mdsauth.dll COM object in Microsoft Windows Media Server in the Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4  
[CVE-2007-2224] Object linking and embedding (OLE) Automation, as used in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Office 2004 for Mac, and Visual Basic 6.0 allows remote attackers to execute arbitrary code via the substringData method on a TextNode object, which causes an integer overflow that leads to a buffer overflow.  
  
[CVE-2007-2225] "A component in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle certain HTTP headers when processing MHTML protocol URLs, which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka ""URL Parsing Cross Domain Information Disclosure Vulnerability."""  
  
[CVE-2007-2227] "The MHTML protocol handler in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle Content-Disposition ""notifications,"" which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka ""Content Disposition Parsing Cross Domain Information Disclosure Vulnerability."""  
  
[CVE-2007-2229] "Microsoft Windows Vista uses insecure default permissions for unspecified ""local user information data stores"" in the registry and the file system, which allows local users to obtain sensitive information such as administrative passwords, aka ""Permissive User Information Store ACLs Information Disclosure Vulnerability."""  
  
[CVE-2007-2237] Microsoft Windows Graphics Device Interface (GDI+, GdiPlus.dll) allows context-dependent attackers to cause a denial of service (crash) via an ICO file with an InfoHeader containing a Height of zero, which triggers a divide-by-zero error.  
  
[CVE-2007-2374] Unspecified vulnerability in Microsoft Windows 2000, XP, and Server 2003 allows user-assisted remote attackers to execute arbitrary code via unspecified vectors. NOTE: this information is based upon a vague pre-advisory with no actionable information. However, the advisory is from a reliable source.  
  
[CVE-2007-2528] Buffer overflow in AgRpcCln.dll for Trend Micro ServerProtect 5.58 for Windows before Security Patch 3 Build 1176 allows remote attackers to execute arbitrary code via unknown vectors related to RPC requests. NOTE: this is probably a different vulnerability than CVE-2007-2508.  
  
[CVE-2007-2581] "Multiple cross-site scripting (XSS) vulnerabilities in Microsoft Windows SharePoint Services 3.0 for Windows Server 2003 and Office SharePoint Server 2007 allow remote attackers to inject arbitrary web script or HTML via the PATH\_INFO (query string) in ""every main page,"" as demonstrated by default.aspx."  
  
[CVE-2007-2593] The Terminal Server in Microsoft Windows 2003 Server, when using TLS, allows remote attackers to bypass SSL and self-signed certificate requirements, downgrade the server security, and possibly conduct man-in-the-middle attacks via unspecified vectors, as demonstrated using the Remote Desktop Protocol (RDP) 6.0 client. NOTE: a third party claims that the vendor may have fixed this in approximately 2006.  
  
[CVE-2007-2729] Comodo Firewall Pro 2.4.18.184 and Comodo Personal Firewall 2.3.6.81, and probably older Comodo Firewall versions, do not properly test for equivalence of process identifiers for certain Microsoft Windows API functions in the NT kernel 5.0 and greater, which allows local users to call these functions, and bypass firewall rules or gain privileges, via a modified identifier that is one, two, or three greater than the canonical identifier.  
  
[CVE-2007-2730] Check Point ZoneAlarm Pro before 6.5.737.000 does not properly test for equivalence of process identifiers for certain Microsoft Windows API functions in the NT kernel 5.0 and greater, which allows local users to call these functions, and bypass firewall rules or gain privileges, via a modified identifier that is one, two, or three greater than the canonical identifier.  
  
[CVE-2007-2815] "The ""hit-highlighting"" functionality in webhits.dll in Microsoft Internet Information Services (IIS) Web Server 5.0 only uses Windows NT ACL configuration, which allows remote attackers to bypass NTLM and basic authentication mechanisms and access private web directories via the CiWebhitsfile parameter to null.htw."  
  
[CVE-2007-2954] Multiple stack-based buffer overflows in the Spooler service (nwspool.dll) in Novell Client 4.91 SP2 through SP4 for Windows allow remote attackers to execute arbitrary code via certain long arguments to the (1) RpcAddPrinterDriver, (2) RpcGetPrinterDriverDirectory, and other unspecified RPC requests, aka Novell bug 300870, a different vulnerability than CVE-2006-5854.  
  
[CVE-2007-2966] Buffer overflow in the LHA decompression component in F-Secure anti-virus products for Microsoft Windows and Linux before 20070529 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted LHA archive, related to an integer wrap, a similar issue to CVE-2006-4335.  
  
[CVE-2007-2967] Multiple F-Secure anti-virus products for Microsoft Windows and Linux before 20070522 allow remote attackers to cause a denial of service (file scanning infinite loop) via certain crafted (1) ARJ archives or (2) FSG packed files.  
  
[CVE-2007-2999] Microsoft Windows Server 2003, when time restrictions are in effect for user accounts, generates different error messages for failed login attempts with a valid user name than for those with an invalid user name, which allows context-dependent attackers to determine valid Active Directory account names.  
  
[CVE-2007-3028] "The LDAP service in Windows Active Directory in Microsoft Windows 2000 Server SP4 does not properly check ""the number of convertible attributes"", which allows remote attackers to cause a denial of service (service unavailability) via a crafted LDAP request, related to ""client sent LDAP request logic,"" aka ""Windows Active Directory Denial of Service Vulnerability"". NOTE: this is probably a different issue than CVE-2007-0040."  
  
[CVE-2007-3034] Integer overflow in the AttemptWrite function in Graphics Rendering Engine (GDI) on Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via a crafted metafile (image) with a large record length value, which triggers a heap-based buffer overflow.  
  
[CVE-2007-3035] "Unspecified vulnerability in Microsoft Windows Media Player 7.1, 9, 10, and 11 allows remote attackers to execute arbitrary code via a skin file (WMZ or WMD) with crafted header information that is not properly handled during decompression, aka ""Windows Media Player Code Execution Vulnerability Decompressing Skins."""  
  
[CVE-2007-3036] "Unspecified vulnerability in the (1) Windows Services for UNIX 3.0 and 3.5, and (2) Subsystem for UNIX-based Applications in Microsoft Windows 2000, XP, Server 2003, and Vista allows local users to gain privileges via unspecified vectors related to ""certain setuid binary files."""  
  
[CVE-2007-3037] "Microsoft Windows Media Player 7.1, 9, 10, and 11 allows remote attackers to execute arbitrary code via a skin file (WMZ or WMD) with crafted header information that causes a size mismatch between compressed and decompressed data and triggers a heap-based buffer overflow, aka ""Windows Media Player Code Execution Vulnerability Parsing Skins."""  
  
[CVE-2007-3038] "The Teredo interface in Microsoft Windows Vista and Vista x64 Edition does not properly handle certain network traffic, which allows remote attackers to bypass firewall blocking rules and obtain sensitive information via crafted IPv6 traffic, aka ""Windows Vista Firewall Blocking Rule Information Disclosure Vulnerability."""  
  
[CVE-2007-3040] Stack-based buffer overflow in agentdpv.dll 2.0.0.3425 in Microsoft Agent on Windows 2000 SP4 allows remote attackers to execute arbitrary code via a crafted URL to the Agent (Agent.Control) ActiveX control, which triggers an overflow within the Agent Service (agentsrv.exe) process, a different issue than CVE-2007-1205.  
  
[CVE-2007-3300] Multiple F-Secure anti-virus products for Microsoft Windows and Linux before 20070619 allow remote attackers to bypass scanning via a crafted header in a (1) LHA or (2) RAR archive.  
  
[CVE-2007-3406] "Multiple absolute path traversal vulnerabilities in Microsoft Internet Explorer 6 on Windows XP SP2 allow remote attackers to access arbitrary local files via the file: URI in the (1) src attribute of a (a) bgsound, (b) input, (c) EMBED, (d) img, or (e) script tag  
[CVE-2007-3436] Microsoft MSN Messenger 4.7 on Windows XP allows remote attackers to cause a denial of service (resource consumption) via a flood of SIP INVITE requests to the port specified for voice conversation.  
  
[CVE-2007-3463] "\*\* DISPUTED \*\* Microsoft Windows XP SP2 allows local users, who have sessions created by another user's RunAs (run as) command, to kill arbitrary processes of this other user, as demonstrated by the taskkill program. NOTE: the researcher claims a vendor dispute in which the vendor states that ""RunAs and UAC are convenience features, not security boundaries. If you need a security guarantee, please log out and log back in with a different account."""  
  
[CVE-2007-3509] Heap-based buffer overflow in the RPC subsystem in Symantec Backup Exec for Windows Servers 10.0, 10d, and 11d allows remote attackers to cause a denial of service (process exit) and possibly execute arbitrary code via crafted ncacn\_ip\_tcp requests.  
  
[CVE-2007-3671] "Unspecified vulnerability in the kernel in Microsoft Windows Vista has unspecified remote attack vectors and impact, as shown in the ""0day IPO"" presentation at SyScan'07."  
  
[CVE-2007-3724] "The process scheduler in the Microsoft Windows XP kernel does not make use of the process statistics kept by the kernel, performs scheduling based on CPU billing gathered from periodic process sampling ticks, and gives preference to ""interactive"" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in ""Secretly Monopolizing the CPU Without Superuser Privileges."""  
  
[CVE-2007-3826] Microsoft Internet Explorer 7 on Windows XP SP2 allows remote attackers to prevent users from leaving a site, spoof the address bar, and conduct phishing and other attacks via repeated document.open function calls after a user requests a new page, but before the onBeforeUnload function is called.  
  
[CVE-2007-3896] "The URL handling in Shell32.dll in the Windows shell in Microsoft Windows XP and Server 2003, with Internet Explorer 7 installed, allows remote attackers to execute arbitrary programs via invalid ""%"" sequences in a mailto: or other URI handler, as demonstrated using mIRC, Outlook, Firefox, Adobe Reader, Skype, and other applications. NOTE: this issue might be related to other issues involving URL handlers in Windows systems, such as CVE-2007-3845. There also might be separate but closely related issues in the applications that are invoked by the handlers."  
  
[CVE-2007-3897] Heap-based buffer overflow in Microsoft Outlook Express 6 and earlier, and Windows Mail for Vista, allows remote Network News Transfer Protocol (NNTP) servers to execute arbitrary code via long NNTP responses that trigger memory corruption.  
  
[CVE-2007-3898] The DNS server in Microsoft Windows 2000 Server SP4, and Server 2003 SP1 and SP2, uses predictable transaction IDs when querying other DNS servers, which allows remote attackers to spoof DNS replies, poison the DNS cache, and facilitate further attack vectors.  
  
[CVE-2007-3958] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service via a certain GIF file, as demonstrated by Art.gif.  
  
[CVE-2007-4218] "Multiple buffer overflows in the ServerProtect service (SpntSvc.exe) in Trend Micro ServerProtect for Windows before 5.58 Security Patch 4 allow remote attackers to execute arbitrary code via certain RPC requests to certain TCP ports that are processed by the (1) RPCFN\_ENG\_NewManualScan, (2) RPCFN\_ENG\_TimedNewManualScan, and (3) RPCFN\_SetComputerName functions in (a) StRpcSrv.dll  
[CVE-2007-4219] Integer overflow in the RPCFN\_SYNC\_TASK function in StRpcSrv.dll, as used by the ServerProtect service (SpntSvc.exe), in Trend Micro ServerProtect for Windows before 5.58 Security Patch 4 allows remote attackers to execute arbitrary code via a certain integer field in a request packet to TCP port 5168, which triggers a heap-based buffer overflow.  
  
[CVE-2007-4227] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service via a certain JPG file, as demonstrated by something.jpg. NOTE: this issue might be related to CVE-2007-3958.  
  
[CVE-2007-4247] Windows Calendar on Microsoft Windows Vista allows remote attackers to cause a denial of service (NULL dereference and persistent application crash) via a malformed ICS file.  
  
[CVE-2007-4288] Microsoft Windows Media Player 11 (wmplayer.exe) allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted .au file that triggers a divide-by-zero error, as demonstrated by iapetus.au.  
  
[CVE-2007-4414] "Cisco VPN Client on Windows before 4.8.02.0010 allows local users to gain privileges by enabling the ""Start Before Logon"" (SBL) and Microsoft Dial-Up Networking options, and then interacting with the dial-up networking dialog box."  
  
[CVE-2007-4490] Multiple buffer overflows in EarthAgent.exe in Trend Micro ServerProtect 5.58 for Windows before Security Patch 4 allow remote attackers to have an unknown impact via certain RPC function calls to (1) RPCFN\_EVENTBACK\_DoHotFix or (2) CMD\_CHANGE\_AGENT\_REGISTER\_INFO.  
  
[CVE-2007-5095] Microsoft Windows Media Player (WMP) 9 on Windows XP SP2 invokes Internet Explorer to render HTML documents contained inside some media files, regardless of what default web browser is configured, which might allow remote attackers to exploit vulnerabilities in software that the user does not expect to run, as demonstrated by the HTMLView parameter in an .asx file.  
  
[CVE-2007-5133] Microsoft Windows Explorer (explorer.exe) allows user-assisted remote attackers to cause a denial of service (CPU consumption) via a certain PNG file with a large tEXt chunk that possibly triggers an integer overflow in PNG chunk size handling, as demonstrated by badlycrafted.png.  
  
[CVE-2007-5145] Multiple buffer overflows in system DLL files in Microsoft Windows XP, as used by Microsoft Windows Explorer (explorer.exe) 6.00.2900.2180, Don Ho Notepad++, unspecified Adobe Macromedia applications, and other programs, allow user-assisted remote attackers to cause a denial of service (application crash) via long strings in the (1) author, (2) title, (3) subject, and (4) comment Properties fields of a file, possibly involving improper handling of extended file attributes by the (a) NtQueryInformationFile, (b) NtQueryDirectoryFile, (c) NtSetInformationFile, (d) FileAllInformation, (e) FileNameInformation, and other FILE\_INFORMATION\_CLASS functions in ntdll.dll and the (f) GetFileAttributesExW and (g) GetFileAttributesW functions in kernel32.dll, a related issue to CVE-2007-1347.  
  
[CVE-2007-5348] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via an image file with crafted gradient sizes in gradient fill input, which triggers a heap-based buffer overflow related to GdiPlus.dll and VGX.DLL, aka ""GDI+ VML Buffer Overrun Vulnerability."""  
  
[CVE-2007-5350] "Unspecified vulnerability in the Windows Advanced Local Procedure Call (ALPC) in the kernel in Microsoft Windows Vista allows local users to gain privileges via unspecified vectors involving ""legacy reply paths."""  
  
[CVE-2007-5351] "Unspecified vulnerability in Server Message Block Version 2 (SMBv2) signing support in Microsoft Windows Vista allows remote attackers to force signature re-computation and execute arbitrary code via a crafted SMBv2 packet, aka ""SMBv2 Signing Vulnerability."""  
  
[CVE-2007-5352] Unspecified vulnerability in Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2 allows local users to gain privileges via a crafted local procedure call (LPC) request.  
  
[CVE-2007-5460] Microsoft ActiveSync 4.1, as used in Windows Mobile 5.0, uses weak encryption (XOR obfuscation with a fixed key) when sending the user's PIN/Password over the USB connection from the host to the device, which might make it easier for attackers to decode a PIN/Password obtained by (1) sniffing or (2) spoofing the docking process.  
  
[CVE-2007-5587] Buffer overflow in Macrovision SafeDisc secdrv.sys before 4.3.86.0, as shipped in Microsoft Windows XP SP2, XP Professional x64 and x64 SP2, Server 2003 SP1 and SP2, and Server 2003 x64 and x64 SP2 allows local users to overwrite arbitrary memory locations and gain privileges via a crafted argument to a METHOD\_NEITHER IOCTL, as originally discovered in the wild.  
  
[CVE-2007-5633] Speedfan.sys in Alfredo Milani Comparetti SpeedFan 4.33, when used on Microsoft Windows Vista x64, allows local users to read or write arbitrary MSRs, and gain privileges and load unsigned drivers, via the (1) IOCTL\_RDMSR 0x9C402438 and (2) IOCTL\_WRMSR 0x9C40243C IOCTLs to \Device\speedfan, as demonstrated by an IOCTL\_WRMSR action on MSR\_LSTAR.  
  
[CVE-2007-5634] Speedfan.sys in Alfredo Milani Comparetti SpeedFan 4.33, when used on Microsoft Windows Vista x64, does not properly check a buffer during an IOCTL 0x9c402420 call, which allows local users to cause a denial of service (machine crash) and possibly gain privileges via unspecified vectors.  
  
[CVE-2007-6043] The CryptGenRandom function in Microsoft Windows 2000 generates predictable values, which makes it easier for context-dependent attackers to reduce the effectiveness of cryptographic mechanisms, as demonstrated by attacks on (1) forward security and (2) backward security, related to use of eight instances of the RC4 cipher, and possibly a related issue to CVE-2007-3898.  
  
[CVE-2007-6236] Microsoft Windows Media Player (WMP) allows remote attackers to cause a denial of service (application crash) via a certain AIFF file that triggers a divide-by-zero error, as demonstrated by kr.aiff.  
  
[CVE-2007-6332] The HPInfoDLL.HPInfo.1 ActiveX control in HPInfoDLL.dll 1.0, as shipped with HP Info Center (hpinfocenter.exe) 1.0.1.1 in HP Quick Launch Button (QLBCTRL.exe, aka QLB) 6.3 and earlier, on Microsoft Windows before Vista allows remote attackers to create or modify arbitrary registry values via the arguments to the SetRegValue method.  
  
[CVE-2007-6401] Stack-based buffer overflow in mplayer2.exe in Microsoft Windows Media Player (WMP) 6.4, when used with the 3ivx 4.5.1 or 5.0.1 codec, allows remote attackers to execute arbitrary code via a certain .mp4 file, possibly a related issue to CVE-2007-6402.  
  
[CVE-2007-6507] "SpntSvc.exe daemon in Trend Micro ServerProtect 5.58 for Windows, before Security Patch 4, exposes unspecified dangerous sub-functions from StRpcSrv.dll in the DCE/RPC interface, which allows remote attackers to obtain ""full file system access"" and execute arbitrary code."  
  
[CVE-2007-6701] Multiple stack-based buffer overflows in the Spooler service (nwspool.dll) in Novell Client 4.91 SP4 for Windows allow remote attackers to execute arbitrary code via long arguments to multiple unspecified RPC functions, aka Novell bug 287919, a different vulnerability than CVE-2007-2954.  
  
[CVE-2007-6753] Untrusted search path vulnerability in Shell32.dll in Microsoft Windows 2000, Windows XP, Windows Vista, Windows Server 2008, and Windows 7, when using an environment configured with a string such as %APPDATA% or %PROGRAMFILES% in a certain way, allows local users to gain privileges via a Trojan horse DLL under the current working directory, as demonstrated by iTunes and Safari.  
  
[CVE-2008-0015] "Stack-based buffer overflow in the CComVariant::ReadFromStream function in the Active Template Library (ATL), as used in the MPEG2TuneRequest ActiveX control in msvidctl.dll in DirectShow, in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted web page, as exploited in the wild in July 2009, aka ""Microsoft Video ActiveX Control Vulnerability."""  
  
[CVE-2008-0020] "Unspecified vulnerability in the Load method in the IPersistStreamInit interface in the Active Template Library (ATL), as used in the Microsoft Video ActiveX control in msvidctl.dll in DirectShow, in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via unknown vectors that trigger memory corruption, aka ""ATL Header Memcopy Vulnerability,"" a different vulnerability than CVE-2008-0015."  
  
[CVE-2008-0080] Heap-based buffer overflow in the WebDAV Mini-Redirector in Microsoft Windows XP SP2, Server 2003 SP1 and SP2, and Vista allows remote attackers to execute arbitrary code via a crafted WebDAV response.  
  
[CVE-2008-0083] The (1) VBScript (VBScript.dll) and (2) JScript (JScript.dll) scripting engines 5.1 and 5.6, as used in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2, do not properly decode script, which allows remote attackers to execute arbitrary code via unknown vectors.  
  
[CVE-2008-0084] Unspecified vulnerability in the TCP/IP support in Microsoft Windows Vista allows remote DHCP servers to cause a denial of service (hang and restart) via a crafted DHCP packet.  
  
[CVE-2008-0087] The DNS client in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, and Vista uses predictable DNS transaction IDs, which allows remote attackers to spoof DNS responses.  
  
[CVE-2008-0088] Unspecified vulnerability in Active Directory on Microsoft Windows 2000 and Windows Server 2003, and Active Directory Application Mode (ADAM) on XP and Server 2003, allows remote attackers to cause a denial of service (hang and restart) via a crafted LDAP request.  
  
[CVE-2008-0322] "The I2O Utility Filter driver (i2omgmt.sys) 5.1.2600.2180 for Microsoft Windows XP sets Everyone/Write permissions for the ""\\.\I2OExc"" device interface, which allows local users to gain privileges. NOTE: this issue can be leveraged to overwrite arbitrary memory and execute code via an IOCTL call with a crafted DeviceObject pointer."  
  
[CVE-2008-0639] Stack-based buffer overflow in the EnumPrinters function in the Spooler service (nwspool.dll) in Novell Client 4.91 SP2, SP3, and SP4 for Windows allows remote attackers to execute arbitrary code via a crafted RPC request, aka Novell bug 353138, a different vulnerability than CVE-2006-5854. NOTE: this issue exists because of an incomplete fix for CVE-2007-6701.  
  
[CVE-2008-0768] Multiple stack-based and heap-based buffer overflows in the Windows RPC components for IBM Informix Storage Manager (ISM), as used in Informix Dynamic Server (IDS) 10.00.xC8 and earlier and 11.10.xC2 and earlier, allow attackers to execute arbitrary code via crafted XDR requests.  
  
[CVE-2008-0951] Microsoft Windows Vista does not properly enforce the NoDriveTypeAutoRun registry value, which allows user-assisted remote attackers, and possibly physically proximate attackers, to execute arbitrary code by inserting a (1) CD-ROM device or (2) U3-enabled USB device containing a filesystem with an Autorun.inf file, and possibly other vectors related to (a) AutoRun and (b) AutoPlay actions.  
  
[CVE-2008-1083] "Heap-based buffer overflow in the CreateDIBPatternBrushPt function in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF or WMF image file with a malformed header that triggers an integer overflow, aka ""GDI Heap Overflow Vulnerability."""  
  
[CVE-2008-1084] Unspecified vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, through Vista SP1, and Server 2008 allows local users to execute arbitrary code via unknown vectors related to improper input validation. NOTE: it was later reported that one affected function is NtUserFnOUTSTRING in win32k.sys.  
  
[CVE-2008-1086] The HxTocCtrl ActiveX control (hxvz.dll), as used in Microsoft Internet Explorer 5.01 SP4 and 6 SP1, in Windows XP SP2, Server 2003 SP1 and SP2, Vista SP1, and Server 2008, allows remote attackers to execute arbitrary code via malformed arguments, which triggers memory corruption.  
  
[CVE-2008-1087] "Stack-based buffer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, and Server 2008 allows remote attackers to execute arbitrary code via an EMF image file with crafted filename parameters, aka ""GDI Stack Overflow Vulnerability."""  
  
[CVE-2008-1435] "Windows Explorer in Microsoft Windows Vista up to SP1, and Server 2008, allows user-assisted remote attackers to execute arbitrary code via crafted saved-search (.search-ms) files that are not properly handled when saving, aka ""Windows Saved Search Vulnerability."""  
  
[CVE-2008-1436] Microsoft Windows XP Professional SP2, Vista, and Server 2003 and 2008 does not properly assign activities to the (1) NetworkService and (2) LocalService accounts, which might allow context-dependent attackers to gain privileges by using one service process to capture a resource from a second service process that has a LocalSystem privilege-escalation ability, related to improper management of the SeImpersonatePrivilege user right, as originally reported for Internet Information Services (IIS), aka Token Kidnapping.  
  
[CVE-2008-1440] "Microsoft Windows XP SP2 and SP3, and Server 2003 SP1 and SP2, does not properly validate the option length field in Pragmatic General Multicast (PGM) packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted PGM packet, aka the ""PGM Invalid Length Vulnerability."""  
  
[CVE-2008-1441] "Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system hang) via a series of Pragmatic General Multicast (PGM) packets with invalid fragment options, aka the ""PGM Malformed Fragment Vulnerability."""  
  
[CVE-2008-1444] "Stack-based buffer overflow in Microsoft DirectX 7.0 and 8.1 on Windows 2000 SP4 allows remote attackers to execute arbitrary code via a Synchronized Accessible Media Interchange (SAMI) file with crafted parameters for a Class Name variable, aka the ""SAMI Format Parsing Vulnerability."""  
  
[CVE-2008-1445] Active Directory on Microsoft Windows 2000 Server SP4, XP Professional SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to cause a denial of service (system hang or reboot) via a crafted LDAP request.  
  
[CVE-2008-1446] "Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka ""Integer Overflow in IPP Service Vulnerability."""  
  
[CVE-2008-1448] "The MHTML protocol handler in a component of Microsoft Outlook Express 5.5 SP2 and 6 through SP1, and Windows Mail, does not assign the correct Internet Explorer Security Zone to UNC share pathnames, which allows remote attackers to bypass intended access restrictions and read arbitrary files via an mhtml: URI in conjunction with a redirection, aka ""URL Parsing Cross-Domain Information Disclosure Vulnerability."""  
  
[CVE-2008-1451] "The WINS service on Microsoft Windows 2000 SP4, and Server 2003 SP1 and SP2, does not properly validate data structures in WINS network packets, which allows local users to gain privileges via a crafted packet, aka ""Memory Overwrite Vulnerability."""  
  
[CVE-2008-1453] The Bluetooth stack in Microsoft Windows XP SP2 and SP3, and Vista Gold and SP1, allows physically proximate attackers to execute arbitrary code via a large series of Service Discovery Protocol (SDP) packets.  
  
[CVE-2008-1454] "Unspecified vulnerability in Microsoft DNS in Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 allows remote attackers to conduct cache poisoning attacks via unknown vectors related to accepting ""records from a response that is outside the remote server's authority,"" aka ""DNS Cache Poisoning Vulnerability,"" a different vulnerability than CVE-2008-1447."  
  
[CVE-2008-1456] Array index vulnerability in the Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote authenticated users to execute arbitrary code via a crafted event subscription request that is used to access an array of function pointers.  
  
[CVE-2008-1457] The Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate per-user subscriptions, which allows remote authenticated users to execute arbitrary code via a crafted event subscription request.  
  
[CVE-2008-1888] Cross-site scripting (XSS) vulnerability in Microsoft Windows SharePoint Services 2.0 allows remote attackers to inject arbitrary web script or HTML via the Picture Source (aka picture object source) field in the Rich Text Editor.  
  
[CVE-2008-2160] Multiple unspecified vulnerabilities in the JPEG (GDI+) and GIF image processing in Microsoft Windows CE 5.0 allow remote attackers to execute arbitrary code via crafted (1) JPEG and (2) GIF images.  
  
[CVE-2008-2245] Heap-based buffer overflow in the InternalOpenColorProfile function in mscms.dll in Microsoft Windows Image Color Management System (MSCMS) in the Image Color Management (ICM) component on Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted image file.  
  
[CVE-2008-2246] Microsoft Windows Vista through SP1 and Server 2008 do not properly import the default IPsec policy from a Windows Server 2003 domain to a Windows Server 2008 domain, which prevents IPsec rules from being enforced and allows remote attackers to bypass intended access restrictions.  
  
[CVE-2008-2249] "Integer overflow in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a malformed header in a crafted WMF file, which triggers a buffer overflow, aka ""GDI Integer Overflow Vulnerability."""  
  
[CVE-2008-2250] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate window properties sent from a parent window to a child window during creation of a new window, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Window Creation Vulnerability."""  
  
[CVE-2008-2251] "Double free vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that makes system calls within multiple threads, aka ""Windows Kernel Unhandled Exception Vulnerability."" NOTE: according to Microsoft, this is not a duplicate of CVE-2008-4510."  
  
[CVE-2008-2252] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate parameters sent from user mode to the kernel, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability."""  
  
[CVE-2008-2253] "Unspecified vulnerability in Microsoft Windows Media Player 11 allows remote attackers to execute arbitrary code via a crafted audio-only file that is streamed from a Server-Side Playlist (SSPL) on Windows Media Server, aka ""Windows Media Player Sampling Rate Vulnerability."""  
  
[CVE-2008-2540] "Apple Safari on Mac OS X, and before 3.1.2 on Windows, does not prompt the user before downloading an object that has an unrecognized content type, which allows remote attackers to place malware into the (1) Desktop directory on Windows or (2) Downloads directory on Mac OS X, and subsequently allows remote attackers to execute arbitrary code on Windows by leveraging an untrusted search path vulnerability in (a) Internet Explorer 7 on Windows XP or (b) the SearchPath function in Windows XP, Vista, and Server 2003 and 2008, aka a ""Carpet Bomb"" and a ""Blended Threat Elevation of Privilege Vulnerability,"" a different issue than CVE-2008-1032. NOTE: Apple considers this a vulnerability only because the Microsoft products can load application libraries from the desktop and, as of 20080619, has not covered the issue in an advisory for Mac OS X."  
  
[CVE-2008-2547] Stack-based buffer overflow in msiexec.exe 3.1.4000.1823 and 4.5.6001.22159 in Microsoft Windows Installer allows context-dependent attackers to execute arbitrary code via a long GUID value for the /x (aka /uninstall) option. NOTE: this issue might cross privilege boundaries if msiexec.exe is reachable via components such as ActiveX controls, and might additionally require a separate vulnerability in the control.  
  
[CVE-2008-3008] "Stack-based buffer overflow in the WMEncProfileManager ActiveX control in wmex.dll in Microsoft Windows Media Encoder 9 Series allows remote attackers to execute arbitrary code via a long first argument to the GetDetailsString method, aka ""Windows Media Encoder Buffer Overrun Vulnerability."""  
  
[CVE-2008-3009] "Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1, 9, and 2008 do not properly use the Service Principal Name (SPN) identifier when validating replies to authentication requests, which allows remote servers to execute arbitrary code via vectors that employ NTLM credential reflection, aka ""SPN Vulnerability."""  
  
[CVE-2008-3010] "Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1 and 9 incorrectly associate ISATAP addresses with the Local Intranet zone, which allows remote servers to capture NTLM credentials, and execute arbitrary code through credential-reflection attacks, by sending an authentication request, aka ""ISATAP Vulnerability."""  
  
[CVE-2008-3012] "gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 does not properly perform memory allocation, which allows remote attackers to execute arbitrary code via a malformed EMF image file, aka ""GDI+ EMF Memory Corruption Vulnerability."""  
  
[CVE-2008-3013] "gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed GIF image file containing many extension markers for graphic control extensions and subsequent unknown labels, aka ""GDI+ GIF Parsing Vulnerability."""  
  
[CVE-2008-3014] "Buffer overflow in gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed WMF image file that triggers improper memory allocation, aka ""GDI+ WMF Buffer Overrun Vulnerability."""  
  
[CVE-2008-3068] Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate embedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtain reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Authority Information Access (AIA) extension.  
  
[CVE-2008-3464] "afd.sys in the Ancillary Function Driver (AFD) component in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP1 and SP2 does not properly validate input sent from user mode to the kernel, which allows local users to gain privileges via a crafted application, as demonstrated using crafted pointers and lengths that bypass intended ProbeForRead and ProbeForWrite restrictions, aka ""AFD Kernel Overwrite Vulnerability."""  
  
[CVE-2008-3465] "Heap-based buffer overflow in an API in GDI in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows context-dependent attackers to cause a denial of service or execute arbitrary code via a WMF file with a malformed file-size parameter, which would not be properly handled by a third-party application that uses this API for a copy operation, aka ""GDI Heap Overflow Vulnerability."""  
  
[CVE-2008-3466] "Microsoft Host Integration Server (HIS) 2000, 2004, and 2006 does not limit RPC access to administrative functions, which allows remote attackers to bypass authentication and execute arbitrary programs via a crafted SNA RPC message using opcode 1 or 6 to call the CreateProcess function, aka ""HIS Command Execution Vulnerability."""  
  
[CVE-2008-3636] Integer overflow in the IopfCompleteRequest API in the kernel in Microsoft Windows 2000, XP, Server 2003, and Vista allows context-dependent attackers to gain privileges. NOTE: this issue was originally reported for GEARAspiWDM.sys 2.0.7.5 in Gear Software CD DVD Filter driver before 4.001.7, as used in other products including Apple iTunes and multiple Symantec and Norton products, which allows local users to gain privileges via repeated IoAttachDevice IOCTL calls to \\.\GEARAspiWDMDevice in this GEARAspiWDM.sys. However, the root cause is the integer overflow in the API call itself.  
  
[CVE-2008-3648] nslookup.exe in Microsoft Windows XP SP2 allows user-assisted remote attackers to execute arbitrary code, as demonstrated by an attempted DNS zone transfer, and as exploited in the wild in August 2008.  
  
[CVE-2008-3815] Unspecified vulnerability in Cisco Adaptive Security Appliances (ASA) 5500 Series and PIX Security Appliances 7.0 before 7.0(8)3, 7.1 before 7.1(2)78, 7.2 before 7.2(4)16, 8.0 before 8.0(4)6, and 8.1 before 8.1(1)13, when configured as a VPN using Microsoft Windows NT Domain authentication, allows remote attackers to bypass VPN authentication via unknown vectors.  
  
[CVE-2008-3893] Microsoft Bitlocker in Windows Vista before SP1 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer during boot, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.  
  
[CVE-2008-3957] "The Microsoft Windows Image Acquisition Logger ActiveX control allows remote attackers to force the download of arbitrary files onto a client system via a URL in the first argument to the Open method, in conjunction with a full destination pathname in the first argument to the Save method. NOTE: the provenance of this information is unknown  
[CVE-2008-4023] "Active Directory in Microsoft Windows 2000 SP4 does not properly allocate memory for (1) LDAP and (2) LDAPS requests, which allows remote attackers to execute arbitrary code via a crafted request, aka ""Active Directory Overflow Vulnerability."""  
  
[CVE-2008-4036] "Integer overflow in Memory Manager in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows local users to gain privileges via a crafted application that triggers an erroneous decrement of a variable, related to validation of parameters for Virtual Address Descriptors (VADs) and a ""memory allocation mapping error,"" aka ""Virtual Address Descriptor Elevation of Privilege Vulnerability."""  
  
[CVE-2008-4037] "Microsoft Windows 2000 Gold through SP4, XP Gold through SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote SMB servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, as demonstrated by backrush, aka ""SMB Credential Reflection Vulnerability."" NOTE: some reliable sources report that this vulnerability exists because of an insufficient fix for CVE-2000-0834."  
  
[CVE-2008-4038] "Buffer underflow in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a Server Message Block (SMB) request that contains a filename with a crafted length, aka ""SMB Buffer Underflow Vulnerability."""  
  
[CVE-2008-4071] A certain ActiveX control in Adobe Acrobat 9, when used with Microsoft Windows Vista and Internet Explorer 7, allows remote attackers to cause a denial of service (browser crash) via an src property value with an invalid acroie:// URL.  
  
[CVE-2008-4127] Mshtml.dll in Microsoft Internet Explorer 7 Gold 7.0.5730 and 8 Beta 8.0.6001 on Windows XP SP2 allows remote attackers to cause a denial of service (failure of subsequent image rendering) via a crafted PNG file, related to an infinite loop in the CDwnTaskExec::ThreadExec function.  
  
[CVE-2008-4255] "Heap-based buffer overflow in mscomct2.ocx (aka Windows Common ActiveX control or Microsoft Animation ActiveX control) in Microsoft Visual Basic 6.0, Visual Studio .NET 2002 SP1 and 2003 SP1, Visual FoxPro 8.0 SP1 and 9.0 SP1 and SP2, and Office Project 2003 SP3 and 2007 Gold and SP1 allows remote attackers to execute arbitrary code via an AVI file with a crafted stream length, which triggers an ""allocation error"" and memory corruption, aka ""Windows Common AVI Parsing Overflow Vulnerability."""  
  
[CVE-2008-4261] "Stack-based buffer overflow in Microsoft Internet Explorer 5.01 SP4, 6 SP1 on Windows 2000, and 6 on Windows XP and Server 2003 does not properly handle extraneous data associated with an object embedded in a web page, which allows remote attackers to execute arbitrary code via crafted HTML tags that trigger memory corruption, aka ""HTML Rendering Memory Corruption Vulnerability."""  
  
[CVE-2008-4268] "The Windows Search component in Microsoft Windows Vista Gold and SP1 and Server 2008 does not properly free memory during a save operation for a Windows Search file, which allows remote attackers to execute arbitrary code via a crafted saved-search file, aka ""Windows Saved Search Vulnerability."""  
  
[CVE-2008-4269] "The search-ms protocol handler in Windows Explorer in Microsoft Windows Vista Gold and SP1 and Server 2008 uses untrusted parameter data obtained from incorrect parsing, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka ""Windows Search Parsing Vulnerability."""  
  
[CVE-2008-4295] Microsoft Windows Mobile 6.0 on HTC Wiza 200 and HTC MDA 8125 devices does not properly handle the first attempt to establish a Bluetooth connection to a peer with a long name, which allows remote attackers to cause a denial of service (device reboot) by configuring a Bluetooth device with a long hci name and (1) connecting directly to the Windows Mobile system or (2) waiting for the Windows Mobile system to scan for nearby devices.  
  
[CVE-2008-4323] Windows Explorer in Microsoft Windows XP SP3 allows user-assisted attackers to cause a denial of service (application crash) via a crafted .ZIP file.  
  
[CVE-2008-4327] gdiplus.dll in GDI+ in Microsoft Windows XP SP3 does not properly handle crafted .ico files, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a certain crash.ico file on a web site, and allows user-assisted attackers to cause a denial of service (divide-by-zero error and persistent application crash) via this crash.ico file on the desktop, a different vulnerability than CVE-2007-2237.  
  
[CVE-2008-4510] Microsoft Windows Vista Home and Ultimate Edition SP1 and earlier allows local users to cause a denial of service (page fault and system crash) via multiple attempts to access a virtual address in a PAGE\_NOACCESS memory page.  
  
[CVE-2008-4609] The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.  
  
[CVE-2008-4834] "Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via malformed values of unspecified ""fields inside the SMB packets"" in an NT Trans request, aka ""SMB Buffer Overflow Remote Code Execution Vulnerability."""  
  
[CVE-2008-4835] "SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via malformed values of unspecified ""fields inside the SMB packets"" in an NT Trans2 request, related to ""insufficiently validating the buffer size,"" aka ""SMB Validation Remote Code Execution Vulnerability."""  
  
[CVE-2008-4841] The WordPad Text Converter for Word 97 files in Microsoft Windows 2000 SP4, XP SP2, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted (1) .doc, (2) .wri, or (3) .rtf Word 97 file that triggers memory corruption, as exploited in the wild in December 2008. NOTE: As of 20081210, it is unclear whether this vulnerability is related to a WordPad issue disclosed on 20080925 with a 2008-crash.doc.rar example, but there are insufficient details to be sure.  
  
[CVE-2008-4927] "Microsoft Windows Media Player (WMP) 9.0 through 11 allows user-assisted attackers to cause a denial of service (application crash) via a malformed (1) MIDI or (2) DAT file, related to ""MThd Header Parsing."" NOTE: the provenance of this information is unknown  
[CVE-2008-5044] Race condition in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (crash or hang) via a multi-threaded application that makes many calls to UnhookWindowsHookEx while certain other desktop activity is occurring.  
  
[CVE-2008-5112] The LDAP server in Active Directory in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 responds differently to a failed bind attempt depending on whether the user account exists and is permitted to login, which allows remote attackers to enumerate valid usernames via a series of LDAP bind requests, as demonstrated by ldapuserenum.  
  
[CVE-2008-5179] Unspecified vulnerability in Microsoft Office Communications Server (OCS), Office Communicator, and Windows Live Messenger allows remote attackers to cause a denial of service (crash) via a crafted Real-time Transport Control Protocol (RTCP) receiver report packet.  
  
[CVE-2008-5229] "Stack-based buffer overflow in Microsoft Device IO Control in iphlpapi.dll in Microsoft Windows Vista Gold and SP1 allows local users in the Network Configuration Operator group to gain privileges or cause a denial of service (system crash) via a large invalid PrefixLength to the CreateIpForwardEntry2 method, as demonstrated by a ""route add"" command. NOTE: this issue might not cross privilege boundaries."  
  
[CVE-2008-5232] "Buffer overflow in the CallHTMLHelp method in the Microsoft Windows Media Services ActiveX control in nskey.dll 4.1.00.3917 in Windows Media Services on Microsoft Windows NT and 2000, and Avaya Media and Message Application servers, allows remote attackers to execute arbitrary code via a long argument. NOTE: the provenance of this information is unknown  
[CVE-2008-5415] The LDBserver service in the server in CA ARCserve Backup 11.1 through 12.0 on Windows allows remote attackers to execute arbitrary code via a handle\_t argument to an RPC endpoint in which the argument refers to an incompatible procedure.  
  
[CVE-2008-5745] Integer overflow in quartz.dll in the DirectShow framework in Microsoft Windows Media Player (WMP) 9, 10, and 11, including 11.0.5721.5260, allows remote attackers to cause a denial of service (application crash) via a crafted (1) WAV, (2) SND, or (3) MID file. NOTE: this has been incorrectly reported as a code-execution vulnerability. NOTE: it is not clear whether this issue is related to CVE-2008-4927.  
  
[CVE-2008-5750] Argument injection vulnerability in Microsoft Internet Explorer 8 beta 2 on Windows XP SP3 allows remote attackers to execute arbitrary commands via the --renderer-path option in a chromehtml: URI.  
  
[CVE-2008-5823] An ActiveX control in prtstb06.dll in Microsoft Money 2006, when used with WScript in Windows Script Host (WSH) on Windows Vista, allows remote attackers to cause a denial of service (access violation and application crash) via a zero value for the Startup property.  
  
[CVE-2008-5828] Microsoft Windows Live Messenger Client 8.5.1 and earlier, when MSN Protocol Version 15 (MSNP15) is used over a NAT session, allows remote attackers to discover intranet IP addresses and port numbers by reading the (1) IPv4InternalAddrsAndPorts, (2) IPv4Internal-Addrs, and (3) IPv4Internal-Port header fields.  
  
[CVE-2008-6194] Memory leak in the DNS server in Microsoft Windows allows remote attackers to cause a denial of service (memory consumption) via DNS packets. NOTE: this issue reportedly exists because of an incorrect fix for CVE-2007-3898.  
  
[CVE-2008-6219] nsrexecd.exe in multiple EMC Networker products including EMC NetWorker Server, Storage Node, and Client 7.3.x and 7.4, 7.4.1, 7.4.2, Client and Storage Node for Open VMS 7.3.2 ECO6 and earlier, Module for Microsoft Exchange 5.1 and earlier, Module for Microsoft Applications 2.0 and earlier, Module for Meditech 2.0 and earlier, and PowerSnap 2.4 SP1 and earlier does not properly control the allocation of memory, which allows remote attackers to cause a denial of service (memory exhaustion) via multiple crafted RPC requests.  
  
[CVE-2008-6819] win32k.sys in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (system crash) via vectors related to CreateWindow, TranslateMessage, and DispatchMessage, possibly a race condition between threads, a different vulnerability than CVE-2008-1084. NOTE: some of these details are obtained from third party information.  
  
[CVE-2009-0078] "The Windows Management Instrumentation (WMI) provider in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka ""Windows WMI Service Isolation Vulnerability."""  
  
[CVE-2009-0081] "The graphics device interface (GDI) implementation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate input received from user mode, which allows remote attackers to execute arbitrary code via a crafted (1) Windows Metafile (aka WMF) or (2) Enhanced Metafile (aka EMF) image file, aka ""Windows Kernel Input Validation Vulnerability."""  
  
[CVE-2009-0082] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate handles, which allows local users to gain privileges via a crafted application that triggers unspecified ""actions,"" aka ""Windows Kernel Handle Validation Vulnerability."""  
  
[CVE-2009-0083] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 does not properly handle invalid pointers, which allows local users to gain privileges via an application that triggers use of a crafted pointer, aka ""Windows Kernel Invalid Pointer Vulnerability."""  
  
[CVE-2009-0085] "The Secure Channel (aka SChannel) authentication component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008, when certificate authentication is used, does not properly validate the client's key exchange data in Transport Layer Security (TLS) handshake messages, which allows remote attackers to spoof authentication by crafting a TLS packet based on knowledge of the certificate but not the private key, aka ""SChannel Spoofing Vulnerability."""  
  
[CVE-2009-0086] "Integer underflow in Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote HTTP servers to execute arbitrary code via crafted parameter values in a response, related to error handling, aka ""Windows HTTP Services Integer Underflow Vulnerability."""  
  
[CVE-2009-0087] "Unspecified vulnerability in the Word 6 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2  
[CVE-2009-0089] "Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Vista Gold allows remote web servers to impersonate arbitrary https web sites by using DNS spoofing to ""forward a connection"" to a different https web site that has a valid certificate matching its own domain name, but not a certificate matching the domain name of the host requested by the user, aka ""Windows HTTP Services Certificate Name Mismatch Vulnerability."""  
  
[CVE-2009-0093] "Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not restrict registration of the ""wpad"" hostname, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) feature, and conduct man-in-the-middle attacks by spoofing a proxy server, via a Dynamic Update request for this hostname, aka ""DNS Server Vulnerability in WPAD Registration Vulnerability,"" a related issue to CVE-2007-1692."  
  
[CVE-2009-0094] "The WINS server in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 does not restrict registration of the (1) ""wpad"" and (2) ""isatap"" NetBIOS names, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) features, and conduct man-in-the-middle attacks by spoofing a proxy server or ISATAP route, by registering one of these names in the WINS database, aka ""WPAD WINS Server Registration Vulnerability,"" a related issue to CVE-2007-1692."  
  
[CVE-2009-0119] Buffer overflow in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .chm file.  
  
[CVE-2009-0202] "Array index error in FL21WIN.DLL in the PowerPoint Freelance Windows 2.1 Translator in Microsoft PowerPoint 2000 and 2002 allows remote attackers to execute arbitrary code via a Freelance file with unspecified ""layout information"" that triggers a heap-based buffer overflow."  
  
[CVE-2009-0229] "The Windows Printing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 allows local users to read arbitrary files via a crafted separator page, aka ""Print Spooler Read File Vulnerability."""  
  
[CVE-2009-0231] "The Embedded OpenType (EOT) Font Engine (T2EMBED.DLL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table in a data record that triggers an integer truncation and a heap-based buffer overflow, aka ""Embedded OpenType Font Heap Overflow Vulnerability."""  
  
[CVE-2009-0232] "Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table, aka ""Embedded OpenType Font Integer Overflow Vulnerability."""  
  
[CVE-2009-0233] "The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not reuse cached DNS responses in all applicable situations, which makes it easier for remote attackers to predict transaction IDs and poison caches by simultaneously sending crafted DNS queries and responses, aka ""DNS Server Query Validation Vulnerability."""  
  
[CVE-2009-0234] "The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 does not properly cache crafted DNS responses, which makes it easier for remote attackers to predict transaction IDs and poison caches by sending many crafted DNS queries that trigger ""unnecessary lookups,"" aka ""DNS Server Response Validation Vulnerability."""  
  
[CVE-2009-0235] "Stack-based buffer overflow in the Word 97 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted Word 97 file that triggers memory corruption, related to use of inconsistent integer data sizes for an unspecified length field, aka ""WordPad Word 97 Text Converter Stack Overflow Vulnerability."""  
  
[CVE-2009-0239] "Cross-site scripting (XSS) vulnerability in Windows Search 4.0 for Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows user-assisted remote attackers to inject arbitrary web script or HTML via a crafted file that appears in a preview in a search result, aka ""Script Execution in Windows Search Vulnerability."""  
  
[CVE-2009-0243] "Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutoRun registry values, which allows physically proximate attackers to execute arbitrary code by (1) inserting CD-ROM media, (2) inserting DVD media, (3) connecting a USB device, and (4) connecting a Firewire device  
[CVE-2009-0244] Directory traversal vulnerability in the OBEX FTP Service in the Microsoft Bluetooth stack in Windows Mobile 6 Professional, and probably Windows Mobile 5.0 for Pocket PC and 5.0 for Pocket PC Phone Edition, allows remote authenticated users to list arbitrary directories, and create or read arbitrary files, via a .. (dot dot) in a pathname. NOTE: this can be leveraged for code execution by writing to a Startup folder.  
  
[CVE-2009-0320] "Microsoft Windows XP, Server 2003 and 2008, and Vista exposes I/O activity measurements of all processes, which allows local users to obtain sensitive information, as demonstrated by reading the I/O Other Bytes column in Task Manager (aka taskmgr.exe) to estimate the number of characters that a different user entered at a runas.exe password prompt, related to a ""benchmarking attack."""  
  
[CVE-2009-0341] The shell32 module in Microsoft Internet Explorer 7.0 on Windows XP SP3 might allow remote attackers to execute arbitrary code via a long VALUE attribute in an INPUT element, possibly related to a stack consumption vulnerability.  
  
[CVE-2009-0550] "Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008  
[CVE-2009-0551] "Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 does not properly handle transition errors in a request for one HTTP document followed by a request for a second HTTP document, which allows remote attackers to execute arbitrary code via vectors involving (1) multiple crafted pages on a web site or (2) a web page with crafted inline content such as banner advertisements, aka ""Page Transition Memory Corruption Vulnerability."""  
  
[CVE-2009-0552] "Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 on Windows XP SP2 and SP3, and 6 on Windows Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0553] "Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0554] "Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka ""Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2009-0555] "Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly process Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted audio file that uses the Windows Media Speech codec, aka ""Windows Media Runtime Voice Sample Rate Vulnerability."""  
  
[CVE-2009-1043] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors triggered by clicking on a link, as demonstrated by Nils during a PWN2OWN competition at CanSecWest 2009.  
  
[CVE-2009-1122] "The WebDAV extension in Microsoft Internet Information Services (IIS) 5.0 on Windows 2000 SP4 does not properly decode URLs, which allows remote attackers to bypass authentication, and possibly read or create files, via a crafted HTTP request, aka ""IIS 5.0 WebDAV Authentication Bypass Vulnerability,"" a different vulnerability than CVE-2009-1535."  
  
[CVE-2009-1123] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate changes to unspecified kernel objects, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Desktop Vulnerability."""  
  
[CVE-2009-1124] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate user-mode pointers in unspecified error conditions, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Pointer Validation Vulnerability."""  
  
[CVE-2009-1125] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly validate an argument to an unspecified system call, which allows local users to gain privileges via a crafted application, aka ""Windows Driver Class Registration Vulnerability."""  
  
[CVE-2009-1126] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate the user-mode input associated with the editing of an unspecified desktop parameter, which allows local users to gain privileges via a crafted application, aka ""Windows Desktop Parameter Edit Vulnerability."""  
  
[CVE-2009-1127] "win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not correctly validate an argument to an unspecified system call, which allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka ""Win32k NULL Pointer Dereferencing Vulnerability."""  
  
[CVE-2009-1132] "Heap-based buffer overflow in the Wireless LAN AutoConfig Service (aka Wlansvc) in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed wireless frame, aka ""Wireless Frame Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2009-1133] "Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka ""Remote Desktop Connection Heap Overflow Vulnerability."""  
  
[CVE-2009-1138] "The LDAP service in Active Directory on Microsoft Windows 2000 SP4 does not properly free memory for LDAP and LDAPS requests, which allows remote attackers to execute arbitrary code via a request that uses hexadecimal encoding, whose associated memory is not released, related to a ""DN AttributeValue,"" aka ""Active Directory Invalid Free Vulnerability."" NOTE: this issue is probably a memory leak."  
  
[CVE-2009-1139] "Memory leak in the LDAP service in Active Directory on Microsoft Windows 2000 SP4 and Server 2003 SP2, and Active Directory Application Mode (ADAM) on Windows XP SP2 and SP3 and Server 2003 SP2, allows remote attackers to cause a denial of service (memory consumption and service outage) via (1) LDAP or (2) LDAPS requests with unspecified OID filters, aka ""Active Directory Memory Leak Vulnerability."""  
  
[CVE-2009-1141] "Microsoft Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via unspecified DHTML function calls related to a tr element and the ""insertion, deletion and attributes of a table cell,"" which trigger memory corruption when the window is destroyed, aka ""DHTML Object Memory Corruption Vulnerability."""  
  
[CVE-2009-1216] "Multiple unspecified vulnerabilities in (1) unlzh.c and (2) unpack.c in the gzip libraries in Microsoft Windows Server 2008, Windows Services for UNIX 3.0 and 3.5, and the Subsystem for UNIX-based Applications (SUA)  
[CVE-2009-1217] "Off-by-one error in the GpFont::SetData function in gdiplus.dll in Microsoft GDI+ on Windows XP allows remote attackers to cause a denial of service (stack corruption and application termination) via a crafted EMF file that triggers an integer overflow, as demonstrated by voltage-exploit.emf, aka the ""Microsoft GdiPlus EMF GpFont.SetData integer overflow."""  
  
[CVE-2009-1331] Integer overflow in Microsoft Windows Media Player (WMP) 11.0.5721.5260 allows remote attackers to cause a denial of service (application crash) via a crafted .mid file, as demonstrated by crash.mid.  
  
[CVE-2009-1335] Microsoft Internet Explorer 7 and 8 on Windows XP and Vista allows remote attackers to cause a denial of service (application hang) via a large document composed of unprintable characters, aka MSRC 9011jr.  
  
[CVE-2009-1511] GDI+ in Microsoft Windows XP SP3 allows remote attackers to cause a denial of service (infinite loop) via a PNG file that contains a certain large btChunkLen value.  
  
[CVE-2009-1528] "Microsoft Internet Explorer 6 and 7 for Windows XP SP2 and SP3  
[CVE-2009-1529] "Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1530] "Use-after-free vulnerability in Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1531] "Microsoft Internet Explorer 7 for Windows XP SP2 and SP3  
[CVE-2009-1532] "Microsoft Internet Explorer 8 for Windows XP SP2 and SP3  
[CVE-2009-1533] "Buffer overflow in the Works for Windows document converters in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP3, Office 2007 SP1, and Works 8.5 and 9 allows remote attackers to execute arbitrary code via a crafted Works .wps file that triggers memory corruption, aka ""File Converter Buffer Overflow Vulnerability."""  
  
[CVE-2009-1537] "Unspecified vulnerability in the QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted QuickTime media file, as exploited in the wild in May 2009, aka ""DirectX NULL Byte Overwrite Vulnerability."""  
  
[CVE-2009-1538] "The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 performs updates to pointers without properly validating unspecified data values, which allows remote attackers to execute arbitrary code via a crafted QuickTime media file, aka ""DirectX Pointer Validation Vulnerability."""  
  
[CVE-2009-1539] "The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 does not properly validate unspecified size fields in QuickTime media files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""DirectX Size Validation Vulnerability."""  
  
[CVE-2009-1545] "Unspecified vulnerability in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed header in a crafted AVI file, aka ""Malformed AVI Header Vulnerability."""  
  
[CVE-2009-1546] "Integer overflow in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows allows remote attackers to execute arbitrary code on a Windows 2000 SP4 system via a crafted AVI file, or cause a denial of service on a Windows XP SP2 or SP3, Server 2003 SP2, Vista Gold, SP1, or SP2, or Server 2008 Gold or SP2 system via a crafted AVI file, aka ""AVI Integer Overflow Vulnerability."""  
  
[CVE-2009-1761] The message engine in CA ARCserve Backup r12.0 and r12.0 SP1 for Windows allows remote attackers to cause a denial of service (crash) via (1) an invalid 0x13 message, which is not properly handled in the ASCORE module, or (2) a 0x3B message with invalid stub data that triggers an RPC marshalling error.  
  
[CVE-2009-1808] Microsoft Windows XP SP3 allows local users to cause a denial of service (system crash) by making an SPI\_SETDESKWALLPAPER SystemParametersInfo call with an improperly terminated pvParam argument, followed by an SPI\_GETDESKWALLPAPER SystemParametersInfo call.  
  
[CVE-2009-1920] "The JScript scripting engine 5.1, 5.6, 5.7, and 5.8 in JScript.dll in Microsoft Windows, as used in Internet Explorer, does not properly load decoded scripts into memory before execution, which allows remote attackers to execute arbitrary code via a crafted web site that triggers memory corruption, aka ""JScript Remote Code Execution Vulnerability."""  
  
[CVE-2009-1922] "The Message Queuing (aka MSMQ) service for Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP2, and Vista Gold does not properly validate unspecified IOCTL request data from user mode before passing this data to kernel mode, which allows local users to gain privileges via a crafted request, aka ""MSMQ Null Pointer Vulnerability."""  
  
[CVE-2009-1923] "Heap-based buffer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted WINS replication packet that triggers an incorrect buffer-length calculation, aka ""WINS Heap Overflow Vulnerability."""  
  
[CVE-2009-1924] "Integer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 allows remote WINS replication partners to execute arbitrary code via crafted data structures in a packet, aka ""WINS Integer Overflow Vulnerability."""  
  
[CVE-2009-1925] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly manage state information, which allows remote attackers to execute arbitrary code by sending packets to a listening service, and thereby triggering misinterpretation of an unspecified field as a function pointer, aka ""TCP/IP Timestamps Code Execution Vulnerability."""  
  
[CVE-2009-1926] "Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to cause a denial of service (TCP outage) via a series of TCP sessions that have pending data and a (1) small or (2) zero receive window size, and remain in the FIN-WAIT-1 or FIN-WAIT-2 state indefinitely, aka ""TCP/IP Orphaned Connections Vulnerability."""  
  
[CVE-2009-1928] "Stack consumption vulnerability in the LDAP service in Active Directory on Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2  
[CVE-2009-1929] "Heap-based buffer overflow in the Microsoft Terminal Services Client ActiveX control running RDP 6.1 on Windows XP SP2, Vista SP1 or SP2, or Server 2008 Gold or SP2  
[CVE-2009-1930] "The Telnet service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote Telnet servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, aka ""Telnet Credential Reflection Vulnerability,"" a related issue to CVE-2000-0834."  
  
[CVE-2009-2357] The default configuration of TekRADIUS 3.0 uses the sa account to communicate with Microsoft SQL Server, which makes it easier for remote attackers to obtain privileged access to the database and the underlying Windows operating system.  
  
[CVE-2009-2484] Stack-based buffer overflow in the Win32AddConnection function in modules/access/smb.c in VideoLAN VLC media player 0.9.9, when running on Microsoft Windows, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long smb URI in a playlist file.  
  
[CVE-2009-2494] "The Active Template Library (ATL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via vectors related to erroneous free operations after reading a variant from a stream and deleting this variant, aka ""ATL Object Type Mismatch Vulnerability."""  
  
[CVE-2009-2498] "Microsoft Windows Media Format Runtime 9.0, 9.5, and 11 and Windows Media Services 9.1 and 2008 do not properly parse malformed headers in Advanced Systems Format (ASF) files, which allows remote attackers to execute arbitrary code via a crafted (1) .asf, (2) .wmv, or (3) .wma file, aka ""Windows Media Header Parsing Invalid Free Vulnerability."""  
  
[CVE-2009-2499] "Microsoft Windows Media Format Runtime 9.0, 9.5, and 11  
[CVE-2009-2500] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted WMF image file, aka ""GDI+ WMF Integer Overflow Vulnerability."""  
  
[CVE-2009-2501] "Heap-based buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka ""GDI+ PNG Heap Overflow Vulnerability."""  
  
[CVE-2009-2502] "Buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted TIFF image file, aka ""GDI+ TIFF Buffer Overflow Vulnerability."""  
  
[CVE-2009-2503] "GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Windows Server 2003 SP2, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 does not properly allocate an unspecified buffer, which allows remote attackers to execute arbitrary code via a crafted TIFF image file that triggers memory corruption, aka ""GDI+ TIFF Memory Corruption Vulnerability."""  
  
[CVE-2009-2504] "Multiple integer overflows in unspecified APIs in GDI+ in Microsoft .NET Framework 1.1 SP1, .NET Framework 2.0 SP1 and SP2, Windows XP SP2 and SP3, Windows Server 2003 SP2, Vista Gold and SP1, Server 2008 Gold, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allow remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka ""GDI+ .NET API Vulnerability."""  
  
[CVE-2009-2505] "The Internet Authentication Service (IAS) in Microsoft Windows Vista SP2 and Server 2008 SP2 does not properly validate MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication requests, which allows remote attackers to execute arbitrary code via crafted structures in a malformed request, aka ""Internet Authentication Service Memory Corruption Vulnerability."""  
  
[CVE-2009-2507] "A certain ActiveX control in the Indexing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly process URLs, which allows remote attackers to execute arbitrary programs via unspecified vectors that cause a ""vulnerable binary"" to load and run, aka ""Memory Corruption in Indexing Service Vulnerability."""  
  
[CVE-2009-2508] "The single sign-on implementation in Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly remove credentials at the end of a network session, which allows physically proximate attackers to obtain the credentials of a previous user of the same web browser by using data from the browser's cache, aka ""Single Sign On Spoofing in ADFS Vulnerability."""  
  
[CVE-2009-2509] "Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly validate headers in HTTP requests, which allows remote authenticated users to execute arbitrary code via a crafted request to an IIS web server, aka ""Remote Code Execution in ADFS Vulnerability."""  
  
[CVE-2009-2510] "The CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, as used by Internet Explorer and other applications, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, aka ""Null Truncation in X.509 Common Name Vulnerability,"" a related issue to CVE-2009-2408."  
  
[CVE-2009-2511] "Integer overflow in the CryptoAPI component in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows man-in-the-middle attackers to spoof arbitrary SSL servers and other entities via an X.509 certificate that has a malformed ASN.1 Object Identifier (OID) and was issued by a legitimate Certification Authority, aka ""Integer Overflow in X.509 Object Identifiers Vulnerability."""  
  
[CVE-2009-2513] "The Graphics Device Interface (GDI) in win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Insufficient Data Validation Vulnerability."""  
  
[CVE-2009-2514] "win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not correctly parse font code during construction of a directory-entry table, which allows remote attackers to execute arbitrary code via a crafted Embedded OpenType (EOT) font, aka ""Win32k EOT Parsing Vulnerability."""  
  
[CVE-2009-2515] "Integer underflow in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows local users to gain privileges via a crafted application that triggers an incorrect truncation of a 64-bit integer to a 32-bit integer, aka ""Windows Kernel Integer Underflow Vulnerability."""  
  
[CVE-2009-2516] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly validate data sent from user mode, which allows local users to gain privileges via a crafted PE .exe file that triggers a NULL pointer dereference during chain traversal, aka ""Windows Kernel NULL Pointer Dereference Vulnerability."""  
  
[CVE-2009-2517] "The kernel in Microsoft Windows Server 2003 SP2 does not properly handle unspecified exceptions when an error condition occurs, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2009-2519] "The DHTML Editing Component ActiveX control in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly format HTML markup, which allows remote attackers to execute arbitrary code via a crafted web site that triggers ""system state"" corruption, aka ""DHTML Editing Component ActiveX Control Vulnerability."""  
  
[CVE-2009-2524] "Integer underflow in the NTLM authentication feature in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to cause a denial of service (reboot) via a malformed packet, aka ""Local Security Authority Subsystem Service Integer Overflow Vulnerability."""  
  
[CVE-2009-2525] "Microsoft Windows Media Runtime, as used in DirectShow WMA Voice Codec, Windows Media Audio Voice Decoder, and Audio Compression Manager (ACM), does not properly initialize unspecified functions within compressed audio files, which allows remote attackers to execute arbitrary code via (1) a crafted media file or (2) crafted streaming content, aka ""Windows Media Runtime Heap Corruption Vulnerability."""  
  
[CVE-2009-2526] "Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 do not properly validate fields in SMBv2 packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted packet to the Server service, aka ""SMBv2 Infinite Loop Vulnerability."""  
  
[CVE-2009-2527] "Heap-based buffer overflow in Microsoft Windows Media Player 6.4 allows remote attackers to execute arbitrary code via (1) a crafted ASF file or (2) crafted streaming content, aka ""WMP Heap Overflow Vulnerability."""  
  
[CVE-2009-2532] "Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC do not properly process the command value in an SMB Multi-Protocol Negotiate Request packet, which allows remote attackers to execute arbitrary code via a crafted SMBv2 packet to the Server service, aka ""SMBv2 Command Value Vulnerability."""  
  
[CVE-2009-2544] Directory traversal vulnerability in the Marcelo Costa FileServer component 1.0 for Microsoft Windows Live Messenger and Messenger Plus! Live (MPL) allows remote authenticated users to list arbitrary directories and read arbitrary files via a .. (dot dot) in a pathname.  
  
[CVE-2009-2653] "\*\* DISPUTED \*\* The NtUserConsoleControl function in win32k.sys in Microsoft Windows XP SP2 and SP3, and Server 2003 before SP1, allows local administrators to bypass unspecified ""security software"" and gain privileges via a crafted call that triggers an overwrite of an arbitrary memory location. NOTE: the vendor disputes the significance of this report, stating that 'the Administrator to SYSTEM ""escalation"" is not a security boundary we defend.'"  
  
[CVE-2009-2655] mshtml.dll in Microsoft Internet Explorer 7 and 8 on Windows XP SP3 allows remote attackers to cause a denial of service (application crash) by calling the JavaScript findText method with a crafted Unicode string in the first argument, and only one additional argument, as demonstrated by a second argument of -1.  
  
[CVE-2009-2764] Microsoft Internet Explorer 8.0.7100.0 on Windows 7 RC on the x64 platform allows remote attackers to cause a denial of service (application crash) via a certain DIV element in conjunction with SCRIPT elements that have empty contents and no reference to a valid external script location.  
  
[CVE-2009-3019] Microsoft Internet Explorer 6 on Windows XP SP2 and SP3, and Internet Explorer 7 on Vista, allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls createElement to create an instance of the LI element, and then calls setAttribute to set the value attribute.  
  
[CVE-2009-3020] win32k.sys in Microsoft Windows Server 2003 SP2 allows remote attackers to cause a denial of service (system crash) by referencing a crafted .eot file in the src descriptor of an @font-face Cascading Style Sheets (CSS) rule in an HTML document, possibly related to the Embedded OpenType (EOT) Font Engine, a different vulnerability than CVE-2006-0010, CVE-2009-0231, and CVE-2009-0232. NOTE: some of these details are obtained from third party information.  
  
[CVE-2009-3103] "Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka ""SMBv2 Negotiation Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2009-3126] "Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka ""GDI+ PNG Integer Overflow Vulnerability."""  
  
[CVE-2009-3294] "The popen API function in TSRM/tsrm\_win32.c in PHP before 5.2.11 and 5.3.x before 5.3.1, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) ""e"" or (2) ""er"" string in the second argument (aka mode), possibly related to the \_fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function."  
  
[CVE-2009-3675] "LSASS.exe in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote authenticated users to cause a denial of service (CPU consumption) via a malformed ISAKMP request over IPsec, aka ""Local Security Authority Subsystem Service Resource Exhaustion Vulnerability."""  
  
[CVE-2009-3676] "The SMB client in the kernel in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to cause a denial of service (infinite loop and system hang) via a (1) SMBv1 or (2) SMBv2 response packet that contains (a) an incorrect length value in a NetBIOS header or (b) an additional length field at the end of this response packet, aka ""SMB Client Incomplete Response Vulnerability."""  
  
[CVE-2009-3677] "The Internet Authentication Service (IAS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly verify the credentials in an MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication request, which allows remote attackers to access network resources via a malformed request, aka ""MS-CHAP Authentication Bypass Vulnerability."""  
  
[CVE-2009-3678] "Integer overflow in cdd.dll in the Canonical Display Driver (CDD) in Microsoft Windows Server 2008 R2 and Windows 7 on 64-bit platforms, when the Windows Aero theme is installed, allows context-dependent attackers to cause a denial of service (reboot) or possibly execute arbitrary code via a crafted image file that triggers incorrect data parsing after user-mode data is copied to kernel mode, as demonstrated using ""Browse with Irfanview"" and certain actions on a folder containing a large number of thumbnail images in Resample mode, possibly related to the ATI graphics driver or win32k.sys, aka ""Canonical Display Driver Integer Overflow Vulnerability."""  
  
[CVE-2009-4210] The Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted media content.  
  
[CVE-2009-4309] Heap-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a large size value in a movi record in an IV41 stream in a media file, as demonstrated by an AVI file.  
  
[CVE-2009-4310] Stack-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted compressed video data in an IV41 stream in a media file, leading to many loop iterations, as demonstrated by data in an AVI file.  
  
[CVE-2009-4311] Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Paul Byrne of NGS Software. NOTE: this might overlap CVE-2008-3615.  
  
[CVE-2009-4312] Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Dave Lenoe of Adobe.  
  
[CVE-2009-4313] ir32\_32.dll 3.24.15.3 in the Indeo32 codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to cause a denial of service (heap corruption) or execute arbitrary code via malformed data in a stream in a media file, as demonstrated by an AVI file.  
  
[CVE-2010-0016] "The SMB client implementation in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate response fields, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted response, aka ""SMB Client Pool Corruption Vulnerability."""  
  
[CVE-2010-0017] "Race condition in the SMB client implementation in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code, and in the SMB client implementation in Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows local users to gain privileges, via a crafted SMB Negotiate response, aka ""SMB Client Race Condition Vulnerability."""  
  
[CVE-2010-0018] "Integer overflow in the Embedded OpenType (EOT) Font Engine (t2embed.dll) in Microsoft Windows 2000 SP4  
[CVE-2010-0019] "Microsoft Silverlight 3 before 3.0.50611.0 on Windows, and before 3.0.41130.0 on Mac OS X, does not properly handle pointers, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and framework outage) via a crafted web site, aka ""Microsoft Silverlight Memory Corruption Vulnerability."""  
  
[CVE-2010-0020] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate request fields, which allows remote authenticated users to execute arbitrary code via a malformed request, aka ""SMB Pathname Overflow Vulnerability."""  
  
[CVE-2010-0021] "Multiple race conditions in the SMB implementation in the Server service in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allow remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 Negotiate packet, aka ""SMB Memory Corruption Vulnerability."""  
  
[CVE-2010-0022] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate the share and servername fields in SMB packets, which allows remote attackers to cause a denial of service (system hang) via a crafted packet, aka ""SMB Null Pointer Vulnerability."""  
  
[CVE-2010-0023] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly kill processes after a logout, which allows local users to obtain sensitive information or gain privileges via a crafted application that continues to execute throughout the logout of one user and the login session of the next user, aka ""CSRSS Local Privilege Elevation Vulnerability."""  
  
[CVE-2010-0024] "The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2003 SP2, does not properly parse MX records, which allows remote DNS servers to cause a denial of service (service outage) via a crafted response to a DNS MX record query, aka ""SMTP Server MX Record Vulnerability."""  
  
[CVE-2010-0025] "The SMTP component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Server 2008 Gold, SP2, and R2, and Exchange Server 2000 SP3, does not properly allocate memory for SMTP command replies, which allows remote attackers to read fragments of e-mail messages by sending a series of invalid commands and then sending a STARTTLS command, aka ""SMTP Memory Allocation Vulnerability."""  
  
[CVE-2010-0026] "The Hyper-V server implementation in Microsoft Windows Server 2008 Gold, SP2, and R2 on the x64 platform allows guest OS users to cause a denial of service (host OS hang) via a crafted application that executes a malformed series of machine instructions, aka ""Hyper-V Instruction Set Validation Vulnerability."""  
  
[CVE-2010-0027] "The URL validation functionality in Microsoft Internet Explorer 5.01, 6, 6 SP1, 7 and 8, and the ShellExecute API function in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, does not properly process input parameters, which allows remote attackers to execute arbitrary local programs via a crafted URL, aka ""URL Validation Vulnerability."""  
  
[CVE-2010-0028] "Integer overflow in Microsoft Paint in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted JPEG (.JPG) file, aka ""MS Paint Integer Overflow Vulnerability."""  
  
[CVE-2010-0035] "The Key Distribution Center (KDC) in Kerberos in Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2, when a trust relationship with a non-Windows Kerberos realm exists, allows remote authenticated users to cause a denial of service (NULL pointer dereference and domain controller outage) via a crafted Ticket Granting Ticket (TGT) renewal request, aka ""Kerberos Null Pointer Dereference Vulnerability."""  
  
[CVE-2010-0231] "The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not use a sufficient source of entropy, which allows remote attackers to obtain access to files and other SMB resources via a large number of authentication requests, related to server-generated challenges, certain ""duplicate values,"" and spoofing of an authentication token, aka ""SMB NTLM Authentication Lack of Entropy Vulnerability."""  
  
[CVE-2010-0232] "The kernel in Microsoft Windows NT 3.1 through Windows 7, including Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, when access to 16-bit applications is enabled on a 32-bit x86 platform, does not properly validate certain BIOS calls, which allows local users to gain privileges by crafting a VDM\_TIB data structure in the Thread Environment Block (TEB), and then calling the NtVdmControl function to start the Windows Virtual DOS Machine (aka NTVDM) subsystem, leading to improperly handled exceptions involving the #GP trap handler (nt!KiTrap0D), aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2010-0233] "Double free vulnerability in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Double Free Vulnerability."""  
  
[CVE-2010-0234] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not properly validate a registry-key argument to an unspecified system call, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Null Pointer Vulnerability."""  
  
[CVE-2010-0235] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold does not perform the expected validation before creating a symbolic link, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Symbolic Link Value Vulnerability."""  
  
[CVE-2010-0236] "The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold does not properly allocate memory for the destination key associated with a symbolic-link registry key, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Allocation Vulnerability."""  
  
[CVE-2010-0237] "The kernel in Microsoft Windows 2000 SP4 and XP SP2 and SP3 allows local users to gain privileges by creating a symbolic link from an untrusted registry hive to a trusted registry hive, aka ""Windows Kernel Symbolic Link Creation Vulnerability."""  
  
[CVE-2010-0238] "Unspecified vulnerability in registry-key validation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, and Vista Gold allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Registry Key Vulnerability."""  
  
[CVE-2010-0239] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Router Advertisement packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""ICMPv6 Router Advertisement Vulnerability."""  
  
[CVE-2010-0240] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when a custom network driver is used, does not properly handle local fragmentation of Encapsulating Security Payload (ESP) over UDP packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""Header MDL Fragmentation Vulnerability."""  
  
[CVE-2010-0241] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Route Information packets, which allows remote attackers to execute arbitrary code via crafted packets, aka ""ICMPv6 Route Information Vulnerability."""  
  
[CVE-2010-0242] "The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows remote attackers to cause a denial of service (system hang) via crafted packets with malformed TCP selective acknowledgement (SACK) values, aka ""TCP/IP Selective Acknowledgement Vulnerability."""  
  
[CVE-2010-0249] "Use-after-free vulnerability in Microsoft Internet Explorer 6, 6 SP1, 7, and 8 on Windows 2000 SP4  
[CVE-2010-0250] "Heap-based buffer overflow in DirectShow in Microsoft DirectX, as used in the AVI Filter on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2, and in Quartz on Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, allows remote attackers to execute arbitrary code via an AVI file with a crafted length field in an unspecified video stream, which is not properly handled by the RLE video decompressor, aka ""DirectShow Heap Overflow Vulnerability."""  
  
[CVE-2010-0252] "The Microsoft Data Analyzer ActiveX control (aka the Office Excel ActiveX control for Data Analysis) in max3activex.dll in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to execute arbitrary code via a crafted web page that corrupts the ""system state,"" aka ""Microsoft Data Analyzer ActiveX Control Vulnerability."""  
  
[CVE-2010-0265] "Buffer overflow in Microsoft Windows Movie Maker 2.1, 2.6, and 6.0, and Microsoft Producer 2003, allows remote attackers to execute arbitrary code via a crafted project (.MSWMM) file, aka ""Movie Maker and Producer Buffer Overflow Vulnerability."""  
  
[CVE-2010-0268] "Unspecified vulnerability in the Windows Media Player ActiveX control in Windows Media Player (WMP) 9 on Microsoft Windows 2000 SP4 and XP SP2 and SP3 allows remote attackers to execute arbitrary code via crafted media content, aka ""Media Player Remote Code Execution Vulnerability."""  
  
[CVE-2010-0269] "The SMB client in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for SMB responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Memory Allocation Vulnerability."""  
  
[CVE-2010-0270] "The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate fields in SMB transaction responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Transaction Vulnerability."""  
  
[CVE-2010-0278] A certain ActiveX control in msgsc.14.0.8089.726.dll in Microsoft Windows Live Messenger 2009 build 14.0.8089.726 on Windows Vista and Windows 7 allows remote attackers to cause a denial of service (msnmsgr.exe crash) by calling the ViewProfile method with a crafted argument during an MSN Messenger session.  
  
[CVE-2010-0378] "Use-after-free vulnerability in Adobe Flash Player 6.0.79, as distributed in Microsoft Windows XP SP2 and SP3, allows remote attackers to execute arbitrary code by unloading a Flash object that is currently being accessed by a script, leading to memory corruption, aka a ""Movie Unloading Vulnerability."""  
  
[CVE-2010-0379] "Multiple unspecified vulnerabilities in the Macromedia Flash ActiveX control in Adobe Flash Player 6, as distributed in Microsoft Windows XP SP2 and SP3, might allow remote attackers to execute arbitrary code via unspecified vectors that are not related to the use-after-free ""Movie Unloading Vulnerability"" (CVE-2010-0378). NOTE: due to lack of details, it is not clear whether this overlaps any other CVE item."  
  
[CVE-2010-0476] "The SMB client in Microsoft Windows Server 2003 SP2, Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted SMB transaction response that uses (1) SMBv1 or (2) SMBv2, aka ""SMB Client Response Parsing Vulnerability."""  
  
[CVE-2010-0477] "The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly handle (1) SMBv1 and (2) SMBv2 response packets, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted packet that causes the client to read the entirety of the response, and then improperly interact with the Winsock Kernel (WSK), aka ""SMB Client Message Size Vulnerability."""  
  
[CVE-2010-0478] "Stack-based buffer overflow in nsum.exe in the Windows Media Unicast Service in Media Services for Microsoft Windows 2000 Server SP4 allows remote attackers to execute arbitrary code via crafted packets associated with transport information, aka ""Media Services Stack-based Buffer Overflow Vulnerability."""  
  
[CVE-2010-0480] "Multiple stack-based buffer overflows in the MPEG Layer-3 audio codecs in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to execute arbitrary code via a crafted AVI file, aka ""MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability."""  
  
[CVE-2010-0481] "The kernel in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly translate a registry key's virtual path to its real path, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Virtual Path Parsing Vulnerability."""  
  
[CVE-2010-0482] "The kernel in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate relocation sections of image files, which allows local users to cause a denial of service (reboot) via a crafted file, aka ""Windows Kernel Malformed Image Vulnerability."""  
  
[CVE-2010-0483] "vbscript.dll in VBScript 5.1, 5.6, 5.7, and 5.8 in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, allows user-assisted remote attackers to execute arbitrary code by referencing a (1) local pathname, (2) UNC share pathname, or (3) WebDAV server with a crafted .hlp file in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution involving winhlp32.exe when the F1 key is pressed, aka ""VBScript Help Keypress Vulnerability."""  
  
[CVE-2010-0484] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 ""do not properly validate changes in certain kernel objects,"" which allows local users to execute arbitrary code via vectors related to Device Contexts (DC) and the GetDCEx function, aka ""Win32k Improper Data Validation Vulnerability."""  
  
[CVE-2010-0485] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 Gold and SP2, Windows 7, and Server 2008 R2 ""do not properly validate all callback parameters when creating a new window,"" which allows local users to execute arbitrary code, aka ""Win32k Window Creation Vulnerability."""  
  
[CVE-2010-0486] "The WinVerifyTrust function in Authenticode Signature Verification 5.1, 6.0, and 6.1 in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly use unspecified fields in a file digest, which allows user-assisted remote attackers to execute arbitrary code via a modified (1) Portable Executable (PE) or (2) cabinet (aka .CAB) file that incorrectly appears to have a valid signature, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2010-0487] "The Authenticode Signature verification functionality in cabview.dll in Cabinet File Viewer Shell Extension 5.1, 6.0, and 6.1 in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly use unspecified fields in a file digest, which allows remote attackers to execute arbitrary code via a modified cabinet (aka .CAB) file that incorrectly appears to have a valid signature, aka ""Cabview Corruption Validation Vulnerability."""  
  
[CVE-2010-0718] Buffer overflow in Microsoft Windows Media Player 9 and 11.0.5721.5145 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted .mpg file.  
  
[CVE-2010-0719] An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.  
  
[CVE-2010-0805] "The Tabular Data Control (TDC) ActiveX control in Microsoft Internet Explorer 5.01 SP4, 6 on Windows XP SP2 and SP3, and 6 SP1 allows remote attackers to execute arbitrary code via a long URL (DataURL parameter) that triggers memory corruption in the CTDCCtl::SecurityCHeckDataURL function, aka ""Memory Corruption Vulnerability."""  
  
[CVE-2010-0808] "Microsoft Internet Explorer 6 and 7 on Windows XP and Vista does not prevent script from simulating user interaction with the AutoComplete feature, which allows remote attackers to obtain sensitive form information via a crafted web site, aka ""AutoComplete Information Disclosure Vulnerability."""  
  
[CVE-2010-0810] "The kernel in Microsoft Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, does not properly handle unspecified exceptions, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2010-0811] "Multiple unspecified vulnerabilities in the Microsoft Internet Explorer 8 Developer Tools ActiveX control in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow remote attackers to execute arbitrary code via unknown vectors that ""corrupt the system state,"" aka ""Microsoft Internet Explorer 8 Developer Tools Vulnerability."""  
  
[CVE-2010-0812] "Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allow remote attackers to bypass intended IPv4 source-address restrictions via a mismatched IPv6 source address in a tunneled ISATAP packet, aka ""ISATAP IPv6 Source Address Spoofing Vulnerability."""  
  
[CVE-2010-0818] "The MPEG-4 codec in the Windows Media codecs in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly handle crafted media content with MPEG-4 video encoding, which allows remote attackers to execute arbitrary code via a file in an unspecified ""supported format,"" aka ""MPEG-4 Codec Vulnerability."""  
  
[CVE-2010-0819] "Unspecified vulnerability in the Windows OpenType Compact Font Format (CFF) driver in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users to execute arbitrary code via unknown vectors related to improper validation when copying data from user mode to kernel mode, aka ""OpenType CFF Font Driver Memory Corruption Vulnerability."""  
  
[CVE-2010-0820] "Heap-based buffer overflow in the Local Security Authority Subsystem Service (LSASS), as used in Active Directory in Microsoft Windows Server 2003 SP2 and Windows Server 2008 Gold, SP2, and R2  
[CVE-2010-0917] Stack-based buffer overflow in VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, might allow user-assisted remote attackers to execute arbitrary code via a long string in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution when the F1 key is pressed, a different vulnerability than CVE-2010-0483.  
  
[CVE-2010-1042] "Microsoft Windows Media Player 11 does not properly perform colorspace conversion, which allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted .AVI file. NOTE: the provenance of this information is unknown  
[CVE-2010-1098] The ANI parser in Microsoft Windows before 7 on the x86 platform, as used in Internet Explorer and other applications, allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted biClrUsed value in the BITMAPINFO header of a .ANI file.  
  
[CVE-2010-1117] Heap-based buffer overflow in Internet Explorer 8 on Microsoft Windows 7 allows remote attackers to discover the base address of a Windows .dll file, and possibly have unspecified other impact, via unknown vectors, as demonstrated by Peter Vreugdenhil during a Pwn2Own competition at CanSecWest 2010.  
  
[CVE-2010-1118] Unspecified vulnerability in Internet Explorer 8 on Microsoft Windows 7 allows remote attackers to execute arbitrary code via unknown vectors, possibly related to a use-after-free issue, as demonstrated by Peter Vreugdenhil during a Pwn2Own competition at CanSecWest 2010.  
  
[CVE-2010-1175] "Microsoft Internet Explorer 7.0 on Windows XP and Windows Server 2003 allows remote attackers to have an unspecified impact via a certain XML document that references a crafted web site in the SRC attribute of an image element, related to a ""0day Vulnerability."""  
  
[CVE-2010-1225] "The memory-management implementation in the Virtual Machine Monitor (aka VMM or hypervisor) in Microsoft Virtual PC 2007 Gold and SP1, Virtual Server 2005 Gold and R2 SP1, and Windows Virtual PC does not properly restrict access from the guest OS to memory locations in the VMM work area, which allows context-dependent attackers to bypass certain anti-exploitation protection mechanisms on the guest OS via crafted input to a vulnerable application. NOTE: the vendor reportedly found that only systems with an otherwise vulnerable application are affected, because ""the memory areas accessible from the guest cannot be leveraged to achieve either remote code execution or elevation of privilege and ... no data from the host is exposed to the guest OS."""  
  
[CVE-2010-1255] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 Gold and SP2, Windows 7, and Server 2008 R2 allows local users to execute arbitrary code via vectors related to ""glyph outline information"" and TrueType fonts, aka ""Win32k TrueType Font Parsing Vulnerability."""  
  
[CVE-2010-1263] "Windows Shell and WordPad in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7  
[CVE-2010-1264] "Unspecified vulnerability in Microsoft Windows SharePoint Services 3.0 SP1 and SP2 allows remote attackers to cause a denial of service (hang) via crafted requests to the Help page that cause repeated restarts of the application pool, aka ""Sharepoint Help Page Denial of Service Vulnerability."""  
  
[CVE-2010-1689] The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 uses predictable transaction IDs that are formed by incrementing a previous ID by 1, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.  
  
[CVE-2010-1690] The DNS implementation in smtpsvc.dll before 6.0.2600.5949 in Microsoft Windows 2000 SP4 and earlier, Windows XP SP3 and earlier, Windows Server 2003 SP2 and earlier, Windows Server 2008 SP2 and earlier, Windows Server 2008 R2, Exchange Server 2003 SP3 and earlier, Exchange Server 2007 SP2 and earlier, and Exchange Server 2010 does not verify that transaction IDs of responses match transaction IDs of queries, which makes it easier for man-in-the-middle attackers to spoof DNS responses, a different vulnerability than CVE-2010-0024 and CVE-2010-0025.  
  
[CVE-2010-1734] The SfnINSTRING function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x18d value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.  
  
[CVE-2010-1735] The SfnLOGONNOTIFY function in win32k.sys in the kernel in Microsoft Windows 2000, XP, and Server 2003 allows local users to cause a denial of service (system crash) via a 0x4c value in the second argument (aka the Msg argument) of a PostMessage function call for the DDEMLEvent window.  
  
[CVE-2010-1880] "Unspecified vulnerability in Quartz.dll for DirectShow on Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista SP1, and Server 2008 allows remote attackers to execute arbitrary code via a media file with crafted compression data, aka ""MJPEG Media Decompression Vulnerability."""  
  
[CVE-2010-1882] "Multiple buffer overflows in the MPEG Layer-3 Audio Codec for Microsoft DirectShow in l3codecx.ax in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allow remote attackers to execute arbitrary code via an MPEG Layer-3 audio stream in (1) a crafted media file or (2) crafted streaming content, aka ""MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability."""  
  
[CVE-2010-1883] "Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to execute arbitrary code via a crafted table in an embedded font, aka ""Embedded OpenType Font Integer Overflow Vulnerability."""  
  
[CVE-2010-1885] "The MPC::HexToNum function in helpctr.exe in Microsoft Windows Help and Support Center in Windows XP and Windows Server 2003 does not properly handle malformed escape sequences, which allows remote attackers to bypass the trusted documents whitelist (fromHCP option) and execute arbitrary commands via a crafted hcp:// URL, aka ""Help Center URL Validation Vulnerability."""  
  
[CVE-2010-1886] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2, and Windows 7 allow local users to gain privileges by leveraging access to a process with NetworkService credentials, as demonstrated by TAPI Server, SQL Server, and IIS processes, and related to the Windows Service Isolation feature. NOTE: the vendor states that privilege escalation from NetworkService to LocalSystem does not cross a ""security boundary."""  
  
[CVE-2010-1887] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly validate an unspecified system-call argument, which allows local users to cause a denial of service (system hang) via a crafted application, aka ""Win32k Bounds Checking Vulnerability."""  
  
[CVE-2010-1888] "Race condition in the kernel in Microsoft Windows XP SP3 allows local users to gain privileges via vectors involving thread creation, aka ""Windows Kernel Data Initialization Vulnerability."""  
  
[CVE-2010-1889] "Double free vulnerability in the kernel in Microsoft Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2, allows local users to gain privileges via a crafted application, related to object initialization during error handling, aka ""Windows Kernel Double Free Vulnerability."""  
  
[CVE-2010-1890] "The kernel in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate ACLs on kernel objects, which allows local users to cause a denial of service (reboot) via a crafted application, aka ""Windows Kernel Improper Validation Vulnerability."""  
  
[CVE-2010-1891] "The Client/Server Runtime Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2, when a Chinese, Japanese, or Korean locale is enabled, does not properly allocate memory for transactions, which allows local users to gain privileges via a crafted application, aka ""CSRSS Local Elevation of Privilege Vulnerability."""  
  
[CVE-2010-1892] "The TCP/IP stack in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly handle malformed IPv6 packets, which allows remote attackers to cause a denial of service (system hang) via multiple crafted packets, aka ""IPv6 Memory Corruption Vulnerability."""  
  
[CVE-2010-1893] "Integer overflow in the TCP/IP stack in Microsoft Windows Vista SP1, Windows Server 2008 Gold and R2, and Windows 7 allows local users to gain privileges via a buffer of user-mode data that is copied to kernel mode, aka ""Integer Overflow in Windows Networking Vulnerability."""  
  
[CVE-2010-1894] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, do not properly handle unspecified exceptions, which allows local users to gain privileges via a crafted application, aka ""Win32k Exception Handling Vulnerability."""  
  
[CVE-2010-1895] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, do not properly perform memory allocation before copying user-mode data to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Win32k Pool Overflow Vulnerability."""  
  
[CVE-2010-1896] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 do not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Win32k User Input Validation Vulnerability."""  
  
[CVE-2010-1897] "The Windows kernel-mode drivers in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly validate pseudo-handle values in callback parameters during window creation, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Creation Vulnerability."""  
  
[CVE-2010-1898] "The Common Language Runtime (CLR) in Microsoft .NET Framework 2.0 SP1, 2.0 SP2, 3.5, 3.5 SP1, and 3.5.1, and Microsoft Silverlight 2 and 3 before 3.0.50611.0 on Windows and before 3.0.41130.0 on Mac OS X, does not properly handle interfaces and delegations to virtual methods, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (aka XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka ""Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability."""  
  
[CVE-2010-2091] Microsoft Outlook Web Access (OWA) 8.2.254.0, when Internet Explorer 7 on Windows Server 2003 is used, does not properly handle the id parameter in a Folder IPF.Note action to the default URI, which might allow remote attackers to obtain sensitive information or conduct cross-site scripting (XSS) attacks via an invalid value.  
  
[CVE-2010-2265] Cross-site scripting (XSS) vulnerability in the GetServerName function in sysinfo/commonFunc.js in Microsoft Windows Help and Support Center for Windows XP and Windows Server 2003 allows remote attackers to inject arbitrary web script or HTML via the svr parameter to sysinfo/sysinfomain.htm. NOTE: this can be leveraged with CVE-2010-1885 to execute arbitrary commands without user interaction.  
  
[CVE-2010-2549] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2 and Server 2008 Gold and SP2 allows local users to gain privileges or cause a denial of service (system crash) by using a large number of calls to the NtUserCheckAccessForIntegrityLevel function to trigger a failure in the LockProcessByClientId function, leading to deletion of an in-use process object, aka ""Win32k Reference Count Vulnerability."""  
  
[CVE-2010-2550] "The SMB Server in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate fields in an SMB request, which allows remote attackers to execute arbitrary code via a crafted SMB packet, aka ""SMB Pool Overflow Vulnerability."""  
  
[CVE-2010-2551] "The SMB Server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate an internal variable in an SMB packet, which allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 packet, aka ""SMB Variable Validation Vulnerability."""  
  
[CVE-2010-2552] "Stack consumption vulnerability in the SMB Server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote attackers to cause a denial of service (system hang) via a malformed SMBv2 compounded request, aka ""SMB Stack Exhaustion Vulnerability."""  
  
[CVE-2010-2553] "The Cinepak codec in Microsoft Windows XP SP2 and SP3, Windows Vista SP1 and SP2, and Windows 7 does not properly decompress media files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""Cinepak Codec Decompression Vulnerability."""  
  
[CVE-2010-2554] "The Tracing Feature for Services in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 has incorrect ACLs on its registry keys, which allows local users to gain privileges via vectors involving a named pipe and impersonation, aka ""Tracing Registry Key ACL Vulnerability."""  
  
[CVE-2010-2555] "The Tracing Feature for Services in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the length of strings in the registry, which allows local users to gain privileges or cause a denial of service (memory corruption) via vectors involving a long string, aka ""Tracing Memory Corruption Vulnerability."""  
  
[CVE-2010-2563] "The Word 97 text converter in the WordPad Text Converters in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly parse malformed structures in Word 97 documents, which allows remote attackers to execute arbitrary code via a crafted document containing an unspecified value that is used in a loop counter, aka ""WordPad Word 97 Text Converter Memory Corruption Vulnerability."""  
  
[CVE-2010-2564] "Buffer overflow in Microsoft Windows Movie Maker (WMM) 2.1, 2.6, and 6.0 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted project file, aka ""Movie Maker Memory Corruption Vulnerability."""  
  
[CVE-2010-2566] "The Secure Channel (aka SChannel) security package in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, does not properly validate certificate request messages from TLS and SSL servers, which allows remote servers to execute arbitrary code via a crafted SSL response, aka ""SChannel Malformed Certificate Request Remote Code Execution Vulnerability."""  
  
[CVE-2010-2568] Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.  
  
[CVE-2010-2731] "Unspecified vulnerability in Microsoft Internet Information Services (IIS) 5.1 on Windows XP SP3, when directory-based Basic Authentication is enabled, allows remote attackers to bypass intended access restrictions and execute ASP files via a crafted request, aka ""Directory Authentication Bypass Vulnerability."""  
  
[CVE-2010-2738] "The Uniscribe (aka new Unicode Script Processor) implementation in USP10.DLL in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2, and Microsoft Office XP SP3, 2003 SP3, and 2007 SP2, does not properly validate tables associated with malformed OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) Office document, aka ""Uniscribe Font Parsing Engine Memory Corruption Vulnerability."""  
  
[CVE-2010-2739] Buffer overflow in the CreateDIBPalette function in win32k.sys in Microsoft Windows XP SP3, Server 2003 R2 Enterprise SP2, Vista Business SP1, Windows 7, and Server 2008 SP2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code by performing a clipboard operation (GetClipboardData API function) with a crafted bitmap with a palette that contains a large number of colors.  
  
[CVE-2010-2740] "The OpenType Font (OTF) format driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly perform memory allocation during font parsing, which allows local users to gain privileges via a crafted application, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2010-2741] "The OpenType Font (OTF) format driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 performs an incorrect integer calculation during font processing, which allows local users to gain privileges via a crafted application, aka ""OpenType Font Validation Vulnerability."""  
  
[CVE-2010-2743] "The kernel-mode drivers in Microsoft Windows XP SP3 do not properly perform indexing of a function-pointer table during the loading of keyboard layouts from disk, which allows local users to gain privileges via a crafted application, as demonstrated in the wild in July 2010 by the Stuxnet worm, aka ""Win32k Keyboard Layout Vulnerability."" NOTE: this might be a duplicate of CVE-2010-3888 or CVE-2010-3889."  
  
[CVE-2010-2744] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 do not properly manage a window class, which allows local users to gain privileges by creating a window, then using (1) the SetWindowLongPtr function to modify the popup menu structure, or (2) the SwitchWndProc function with a switch window information pointer, which is not re-initialized when a WM\_NCCREATE message is processed, aka ""Win32k Window Class Vulnerability."""  
  
[CVE-2010-2745] "Microsoft Windows Media Player (WMP) 9 through 12 does not properly deallocate objects during a browser reload action, which allows user-assisted remote attackers to execute arbitrary code via crafted media content referenced in an HTML document, aka ""Windows Media Player Memory Corruption Vulnerability."""  
  
[CVE-2010-2746] "Heap-based buffer overflow in Comctl32.dll (aka the common control library) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when a third-party SVG viewer is used, allows remote attackers to execute arbitrary code via a crafted HTML document that triggers unspecified messages from this viewer, aka ""Comctl32 Heap Overflow Vulnerability."""  
  
[CVE-2010-3138] "Untrusted search path vulnerability in the Indeo Codec in iac25\_32.ax in Microsoft Windows XP SP3 allows local users to gain privileges via a Trojan horse iacenc.dll file in the current working directory, as demonstrated by access through BS.Player or Media Player Classic to a directory that contains a .avi, .mka, .ra, or .ram file, aka ""Indeo Codec Insecure Library Loading Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2010-3140] Untrusted search path vulnerability in Microsoft Windows Internet Communication Settings on Windows XP SP3 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse schannel.dll that is located in the same folder as an ISP file.  
  
[CVE-2010-3143] Untrusted search path vulnerability in Microsoft Windows Contacts allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse wab32res.dll that is located in the same folder as a .contact, .group, .p7c, .vcf, or .wab file. NOTE: the codebase for this product may overlap the codebase for the product referenced in CVE-2010-3147.  
  
[CVE-2010-3144] "Untrusted search path vulnerability in the Internet Connection Signup Wizard in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse smmscrpt.dll file in the current working directory, as demonstrated by a directory that contains an ISP or INS file, aka ""Internet Connection Signup Wizard Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3145] "Untrusted search path vulnerability in the BitLocker Drive Encryption API, as used in sdclt.exe in Backup Manager in Microsoft Windows Vista SP1 and SP2, allows local users to gain privileges via a Trojan horse fveapi.dll file in the current working directory, as demonstrated by a directory that contains a Windows Backup Catalog (.wbcat) file, aka ""Backup Manager Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3147] "Untrusted search path vulnerability in wab.exe 6.00.2900.5512 in Windows Address Book in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a Trojan horse wab32res.dll file in the current working directory, as demonstrated by a directory that contains a Windows Address Book (WAB), VCF (aka vCard), or P7C file, aka ""Insecure Library Loading Vulnerability."" NOTE: the codebase for this product may overlap the codebase for the product referenced in CVE-2010-3143."  
  
[CVE-2010-3223] "The user interface in Microsoft Cluster Service (MSCS) in Microsoft Windows Server 2008 R2 does not properly set administrative-share permissions for new cluster disks that are shared as part of a failover cluster, which allows remote attackers to read or modify data on these disks via requests to the associated share, aka ""Permissions on New Cluster Disks Vulnerability."""  
  
[CVE-2010-3225] "Use-after-free vulnerability in the Media Player Network Sharing Service in Microsoft Windows Vista SP1 and SP2 and Windows 7 allows remote attackers to execute arbitrary code via a crafted Real Time Streaming Protocol (RTSP) packet, aka ""RTSP Use After Free Vulnerability."""  
  
[CVE-2010-3227] "Stack-based buffer overflow in the UpdateFrameTitleForDocument method in the CFrameWnd class in mfc42.dll in the Microsoft Foundation Class (MFC) Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows context-dependent attackers to execute arbitrary code via a long window title that this library attempts to create at the request of an application, as demonstrated by the Trident PowerZip 7.2 Build 4010 application, aka ""Windows MFC Document Title Updating Buffer Overflow Vulnerability."""  
  
[CVE-2010-3229] "The Secure Channel (aka SChannel) security package in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, when IIS 7.x is used, does not properly process client certificates during SSL and TLS handshakes, which allows remote attackers to cause a denial of service (LSASS outage and reboot) via a crafted packet, aka ""TLSv1 Denial of Service Vulnerability."""  
  
[CVE-2010-3243] "Cross-site scripting (XSS) vulnerability in the toStaticHTML function in Microsoft Internet Explorer 8, and the SafeHTML function in Microsoft Windows SharePoint Services 3.0 SP2 and Office SharePoint Server 2007 SP2, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka ""HTML Sanitization Vulnerability."""  
  
[CVE-2010-3324] "The toStaticHTML function in Microsoft Internet Explorer 8, and the SafeHTML function in Microsoft Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010, Office SharePoint Server 2007 SP2, Groove Server 2010, and Office Web Apps, allows remote attackers to bypass the cross-site scripting (XSS) protection mechanism and conduct XSS attacks via a crafted use of the Cascading Style Sheets (CSS) @import rule, aka ""HTML Sanitization Vulnerability,"" a different vulnerability than CVE-2010-1257."  
  
[CVE-2010-3338] "The Windows Task Scheduler in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the security context of scheduled tasks, which allows local users to gain privileges via a crafted application, aka ""Task Scheduler Vulnerability."" NOTE: this might overlap CVE-2010-3888."  
  
[CVE-2010-3888] Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Kaspersky Lab researchers and other researchers.  
  
[CVE-2010-3889] Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Microsoft researchers and other researchers.  
  
[CVE-2010-3937] "Microsoft Exchange Server 2007 SP2 on the x64 platform allows remote authenticated users to cause a denial of service (infinite loop and MSExchangeIS outage) via a crafted RPC request, aka ""Exchange Server Infinite Loop Vulnerability."""  
  
[CVE-2010-3939] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via vectors related to improper memory allocation for copies from user mode, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2010-3940] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted application, aka ""Win32k PFE Pointer Double Free Vulnerability."""  
  
[CVE-2010-3941] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold and SP2, and Windows 7 allows local users to gain privileges via a crafted application, aka ""Win32k Double Free Vulnerability."""  
  
[CVE-2010-3942] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for copies from user mode, which allows local users to gain privileges via a crafted application, aka ""Win32k WriteAV Vulnerability."""  
  
[CVE-2010-3943] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly link driver objects, which allows local users to gain privileges via a crafted application that triggers linked-list corruption, aka ""Win32k Cursor Linking Vulnerability."""  
  
[CVE-2010-3944] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2010-3956] "The OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly perform array indexing, which allows local users to gain privileges via a crafted OpenType font, aka ""OpenType Font Index Vulnerability."""  
  
[CVE-2010-3957] "Double free vulnerability in the OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted OpenType font, aka ""OpenType Font Double Free Vulnerability."""  
  
[CVE-2010-3959] "The OpenType Font (OTF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a crafted CMAP table in an OpenType font, aka ""OpenType CMAP Table Vulnerability."""  
  
[CVE-2010-3960] "Hyper-V in Microsoft Windows Server 2008 Gold, SP2, and R2 allows guest OS users to cause a denial of service (host OS hang) by sending a crafted encapsulated packet over the VMBus, aka ""Hyper-V VMBus Vulnerability."""  
  
[CVE-2010-3961] "The Consent User Interface (UI) in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly handle an unspecified registry-key value, which allows local users with SeImpersonatePrivilege rights to gain privileges via a crafted application, aka ""Consent UI Impersonation Vulnerability."""  
  
[CVE-2010-3963] "Buffer overflow in the Routing and Remote Access NDProxy component in the kernel in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted application, related to the Routing and Remote Access service (RRAS) and improper copying from user mode to the kernel, aka ""Kernel NDProxy Buffer Overflow Vulnerability."""  
  
[CVE-2010-3965] "Untrusted search path vulnerability in Windows Media Encoder 9 on Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Windows Media Profile (PRX) file, aka ""Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3966] "Untrusted search path vulnerability in Microsoft Windows Server 2008 R2 and Windows 7, when BranchCache is supported, allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an EML file, an RSS file, or a WPOST file, aka ""BranchCache Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3967] "Untrusted search path vulnerability in Microsoft Windows Movie Maker (WMM) 2.6 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Movie Maker (MSWMM) file, aka ""Insecure Library Loading Vulnerability."""  
  
[CVE-2010-3970] "Stack-based buffer overflow in the CreateSizedDIBSECTION function in shimgvw.dll in the Windows Shell graphics processor (aka graphics rendering engine) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted .MIC or unspecified Office document containing a thumbnail bitmap with a negative biClrUsed value, as reported by Moti and Xu Hao, aka ""Windows Shell Graphics Processing Overrun Vulnerability."""  
  
[CVE-2010-3973] "The WMITools ActiveX control in WBEMSingleView.ocx 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via a crafted argument to the AddContextRef method, possibly an untrusted pointer dereference, aka ""Microsoft WMITools ActiveX Control Vulnerability."""  
  
[CVE-2010-3974] "fxscover.exe in the Fax Cover Page Editor in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly parse FAX cover pages, which allows remote attackers to execute arbitrary code via a crafted .cov file, aka ""Fax Cover Page Editor Memory Corruption Vulnerability."""  
  
[CVE-2010-4182] "Untrusted search path vulnerability in the Data Access Objects (DAO) library (dao360.dll) in Microsoft Windows XP Professional SP3, Windows Server 2003 R2 Enterprise Edition SP3, Windows Vista Business SP1, and Windows 7 Professional allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse msjet49.dll that is located in the same folder as a file that is processed by dao360.dll. NOTE: the provenance of this information is unknown  
[CVE-2010-4398] "Stack-based buffer overflow in the RtlQueryRegistryValues function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges, and bypass the User Account Control (UAC) feature, via a crafted REG\_BINARY value for a SystemDefaultEUDCFont registry key, aka ""Driver Improper Interaction with Windows Kernel Vulnerability."""  
  
[CVE-2010-4562] Microsoft Windows 2008, 7, Vista, 2003, 2000, and XP, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping. NOTE: due to a typo, some sources map CVE-2010-4562 to a ProFTPd mod\_sql vulnerability, but that issue is covered by CVE-2010-4652.  
  
[CVE-2010-4669] The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 allows remote attackers to cause a denial of service (CPU consumption and system hang) by sending many Router Advertisement (RA) messages with different source addresses, as demonstrated by the flood\_router6 program in the thc-ipv6 package.  
  
[CVE-2010-4701] Heap-based buffer overflow in the CDrawPoly::Serialize function in fxscover.exe in Microsoft Windows Fax Services Cover Page Editor 5.2 r2 in Windows XP Professional SP3, Server 2003 R2 Enterprise Edition SP2, and Windows 7 Professional allows remote attackers to execute arbitrary code via a long record in a Fax Cover Page (.cov) file. NOTE: some of these details are obtained from third party information.  
  
[CVE-2010-5082] "Untrusted search path vulnerability in colorcpl.exe 6.0.6000.16386 in the Color Control Panel in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 allows local users to gain privileges via a Trojan horse sti.dll file in the current working directory, as demonstrated by a directory that contains a .camp, .cdmp, .gmmp, .icc, or .icm file, aka ""Color Control Panel Insecure Library Loading Vulnerability."""  
  
[CVE-2011-0026] "Integer signedness error in the SQLConnectW function in an ODBC API (odbc32.dll) in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, allows remote attackers to execute arbitrary code via a long string in the Data Source Name (DSN) and a crafted szDSN argument, which bypasses a signed comparison and leads to a buffer overflow, aka ""DSN Overflow Vulnerability."""  
  
[CVE-2011-0027] "Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, does not properly validate memory allocation for internal data structures, which allows remote attackers to execute arbitrary code, possibly via a large CacheSize property that triggers an integer wrap and a buffer overflow, aka ""ADO Record Memory Vulnerability."" NOTE: this might be a duplicate of CVE-2010-1117 or CVE-2010-1118."  
  
[CVE-2011-0028] "WordPad in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly parse fields in Word documents, which allows remote attackers to execute arbitrary code via a crafted .doc file, aka ""WordPad Converter Parsing Vulnerability."""  
  
[CVE-2011-0030] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly kill processes after a logout, which allows local users to obtain sensitive information or gain privileges via a crafted application that continues to execute throughout the logout of one user and the login session of the next user, aka ""CSRSS Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2010-0023."  
  
[CVE-2011-0031] "The (1) JScript 5.8 and (2) VBScript 5.8 scripting engines in Microsoft Windows Server 2008 R2 and Windows 7 do not properly load decoded scripts obtained from web pages, which allows remote attackers to trigger memory corruption and consequently obtain sensitive information via a crafted web site, aka ""Scripting Engines Information Disclosure Vulnerability."""  
  
[CVE-2011-0032] "Untrusted search path vulnerability in DirectShow in Microsoft Windows Vista SP1 and SP2, Windows 7 Gold and SP1, Windows Server 2008 R2 and R2 SP1, and Windows Media Center TV Pack for Windows Vista allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a Digital Video Recording (.dvr-ms), Windows Recorded TV Show (.wtv), or .mpg file, aka ""DirectShow Insecure Library Loading Vulnerability."""  
  
[CVE-2011-0033] "The OpenType Compact Font Format (CFF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate parameter values in OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted font, aka ""OpenType Font Encoded Character Vulnerability."""  
  
[CVE-2011-0034] "Stack-based buffer overflow in the OpenType Compact Font Format (aka OTF or CFF) driver in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via crafted parameter values in an OpenType font, aka ""OpenType Font Stack Overflow Vulnerability."""  
  
[CVE-2011-0037] Microsoft Malware Protection Engine before 1.1.6603.0, as used in Microsoft Malicious Software Removal Tool (MSRT), Windows Defender, Security Essentials, Forefront Client Security, Forefront Endpoint Protection 2010, and Windows Live OneCare, allows local users to gain privileges via a crafted value of an unspecified user registry key.  
  
[CVE-2011-0039] "The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly process authentication requests, which allows local users to gain privileges via a request with a crafted length, aka ""LSASS Length Validation Vulnerability."""  
  
[CVE-2011-0040] "The server in Microsoft Active Directory on Windows Server 2003 SP2 does not properly handle an update request for a service principal name (SPN), which allows remote attackers to cause a denial of service (authentication downgrade or outage) via a crafted request that triggers name collisions, aka ""Active Directory SPN Validation Vulnerability."""  
  
[CVE-2011-0041] "Integer overflow in gdiplus.dll in GDI+ in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold and SP2, and Office XP SP3 allows remote attackers to execute arbitrary code via a crafted EMF image, aka ""GDI+ Integer Overflow Vulnerability."""  
  
[CVE-2011-0042] "SBE.dll in the Stream Buffer Engine in Windows Media Player and Windows Media Center in Microsoft Windows XP SP2 and SP3, Windows XP Media Center Edition 2005 SP3, Windows Vista SP1 and SP2, Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista does not properly parse Digital Video Recording (.dvr-ms) files, which allows remote attackers to execute arbitrary code via a crafted file, aka ""DVR-MS Vulnerability."""  
  
[CVE-2011-0043] "Kerberos in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 supports weak hashing algorithms, which allows local users to gain privileges by operating a service that sends crafted service tickets, as demonstrated by the CRC32 algorithm, aka ""Kerberos Unkeyed Checksum Vulnerability."""  
  
[CVE-2011-0045] "The Trace Events functionality in the kernel in Microsoft Windows XP SP3 does not properly perform type conversion, which causes integer truncation and insufficient memory allocation and triggers a buffer overflow, which allows local users to gain privileges via a crafted application, related to WmiTraceMessageVa, aka ""Windows Kernel Integer Truncation Vulnerability."""  
  
[CVE-2011-0086] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Improper User Input Validation Vulnerability."""  
  
[CVE-2011-0087] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Insufficient User Input Validation Vulnerability."""  
  
[CVE-2011-0088] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Class Pointer Confusion Vulnerability."""  
  
[CVE-2011-0089] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Class Improper Pointer Validation Vulnerability."""  
  
[CVE-2011-0090] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2011-0091] "Kerberos in Microsoft Windows Server 2008 R2 and Windows 7 does not prevent a session from changing from strong encryption to DES encryption, which allows man-in-the-middle attackers to spoof network traffic and obtain sensitive information via a DES downgrade, aka ""Kerberos Spoofing Vulnerability."""  
  
[CVE-2011-0096] "The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for content blocks in a document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site that is visited in Internet Explorer, aka ""MHTML Mime-Formatted Request Vulnerability."""  
  
[CVE-2011-0347] Microsoft Internet Explorer on Windows XP allows remote attackers to trigger an incorrect GUI display and have unspecified other impact via vectors related to the DOM implementation, as demonstrated by cross\_fuzz.  
  
[CVE-2011-0627] Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.  
  
[CVE-2011-0638] Microsoft Windows does not properly warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.  
  
[CVE-2011-0654] "Integer underflow in the BowserWriteErrorLogEntry function in the Common Internet File System (CIFS) browser service in Mrxsmb.sys or bowser.sys in Active Directory in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via a malformed BROWSER ELECTION message, leading to a heap-based buffer overflow, aka ""Browser Pool Corruption Vulnerability."" NOTE: some of these details are obtained from third party information."  
  
[CVE-2011-0657] "DNSAPI.dll in the DNS client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process DNS queries, which allows remote attackers to execute arbitrary code via (1) a crafted LLMNR broadcast query or (2) a crafted application, aka ""DNS Query Vulnerability."""  
  
[CVE-2011-0658] "Integer underflow in the OLE Automation protocol implementation in VBScript.dll in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted WMF file, aka ""OLE Automation Underflow Vulnerability."""  
  
[CVE-2011-0660] "The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Client Response Parsing Vulnerability."""  
  
[CVE-2011-0661] "The SMB Server service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet, aka ""SMB Transaction Parsing Vulnerability."""  
  
[CVE-2011-0662] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0665] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0666] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0667] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0670] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0671] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0672] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0673] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-0674] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0675] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-0676] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-0677] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1068] Microsoft Windows Azure Software Development Kit (SDK) 1.3.x before 1.3.20121.1237, when Full IIS and a Web Role are used with an ASP.NET application, does not properly support the use of cookies for maintaining state, which allows remote attackers to obtain potentially sensitive information by reading an encrypted cookie and performing unspecified other steps.  
  
[CVE-2011-1225] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1226] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1227] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1228] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1229] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1230] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1231] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1232] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1233] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other ""Vulnerability Type 2"" CVEs listed in MS11-034, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1234] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1235] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1236] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1237] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1238] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1239] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1240] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1241] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1242] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other ""Vulnerability Type 1"" CVEs listed in MS11-034, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1243] "The Windows Messenger ActiveX control in msgsc.dll in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via unspecified vectors that ""corrupt the system state,"" aka ""Microsoft Windows Messenger ActiveX Control Vulnerability."""  
  
[CVE-2011-1247] "Untrusted search path vulnerability in the Microsoft Active Accessibility component in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Active Accessibility Insecure Library Loading Vulnerability."""  
  
[CVE-2011-1248] "WINS in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1 does not properly handle socket send exceptions, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted packets, related to unintended stack-frame values and buffer passing, aka ""WINS Service Failed Response Vulnerability."""  
  
[CVE-2011-1249] "The Ancillary Function Driver (AFD) in afd.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1252] "Cross-site scripting (XSS) vulnerability in the SafeHTML function in the toStaticHTML API in Microsoft Internet Explorer 7 and 8, Office SharePoint Server 2007 SP2, Office SharePoint Server 2010 Gold and SP1, Groove Server 2010 Gold and SP1, Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1 allows remote attackers to inject arbitrary web script or HTML via unspecified strings, aka ""toStaticHTML Information Disclosure Vulnerability"" or ""HTML Sanitization Vulnerability."""  
  
[CVE-2011-1263] "Cross-site scripting (XSS) vulnerability in the logon page in Remote Desktop Web Access (RD Web Access) in Microsoft Windows Server 2008 R2 and R2 SP1 allows remote attackers to inject arbitrary web script or HTML via the URI, aka ""Remote Desktop Web Access Vulnerability."""  
  
[CVE-2011-1264] "Cross-site scripting (XSS) vulnerability in Active Directory Certificate Services Web Enrollment in Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1 allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka ""Active Directory Certificate Services Vulnerability."""  
  
[CVE-2011-1265] "The Bluetooth Stack 2.1 in Microsoft Windows Vista SP1 and SP2 and Windows 7 Gold and SP1 does not prevent access to objects in memory that (1) were not properly initialized or (2) have been deleted, which allows remote attackers to execute arbitrary code via crafted Bluetooth packets, aka ""Bluetooth Stack Vulnerability."""  
  
[CVE-2011-1267] "The SMB server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 request, aka ""SMB Request Parsing Vulnerability."""  
  
[CVE-2011-1268] "The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka ""SMB Response Parsing Vulnerability."""  
  
[CVE-2011-1281] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly restrict the number of console objects for a process, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP AllocConsole Vulnerability."""  
  
[CVE-2011-1282] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly initialize memory and consequently uses a NULL pointer in an unspecified function call, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvSetConsoleLocalEUDC Vulnerability."""  
  
[CVE-2011-1283] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2 does not ensure that an unspecified array index has a non-negative value before performing read and write operations, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvSetConsoleNumberOfCommand Vulnerability."""  
  
[CVE-2011-1284] "Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvWriteConsoleOutput Vulnerability."""  
  
[CVE-2011-1346] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors, as demonstrated by Stephen Fewer as the second of three chained vulnerabilities during a Pwn2Own competition at CanSecWest 2011.  
  
[CVE-2011-1347] Unspecified vulnerability in Microsoft Internet Explorer 8 on Windows 7 allows remote attackers to bypass Protected Mode and create arbitrary files by leveraging access to a Low integrity process, as demonstrated by Stephen Fewer as the third of three chained vulnerabilities during a Pwn2Own competition at CanSecWest 2011.  
  
[CVE-2011-1652] "\*\* DISPUTED \*\* The default configuration of Microsoft Windows 7 immediately prefers a new IPv6 and DHCPv6 service over a currently used IPv4 and DHCPv4 service upon receipt of an IPv6 Router Advertisement (RA), and does not provide an option to ignore an unexpected RA, which allows remote attackers to conduct man-in-the-middle attacks on communication with external IPv4 servers via vectors involving RAs, a DHCPv6 server, and NAT-PT on the local network, aka a ""SLAAC Attack."" NOTE: it can be argued that preferring IPv6 complies with RFC 3484, and that attempting to determine the legitimacy of an RA is currently outside the scope of recommended behavior of host operating systems."  
  
[CVE-2011-1713] Microsoft msxml.dll, as used in Internet Explorer 8 on Windows 7, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function. NOTE: this might overlap CVE-2011-1202.  
  
[CVE-2011-1868] "The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate fields in DFS responses, which allows remote DFS servers to execute arbitrary code via a crafted response, aka ""DFS Memory Corruption Vulnerability."""  
  
[CVE-2011-1869] "The Distributed File System (DFS) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote DFS servers to cause a denial of service (system hang) via a crafted referral response, aka ""DFS Referral Response Vulnerability."""  
  
[CVE-2011-1870] "Integer overflow in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, and Windows Server 2003 SP2, allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that triggers an incorrect memory assignment for a user transaction, aka ""CSRSS Local EOP SrvWriteConsoleOutputString Vulnerability."""  
  
[CVE-2011-1871] "Tcpip.sys in the TCP/IP stack in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a series of crafted ICMP messages, aka ""ICMP Denial of Service Vulnerability."""  
  
[CVE-2011-1872] "Hyper-V in Microsoft Windows Server 2008 Gold, SP2, R2, and R2 SP1 allows guest OS users to cause a denial of service (host OS infinite loop) via malformed machine instructions in a VMBus packet, aka ""VMBus Persistent DoS Vulnerability."""  
  
[CVE-2011-1873] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 on 64-bit platforms does not properly validate pointers during the parsing of OpenType (aka OTF) fonts, which allows remote attackers to execute arbitrary code via a crafted font file, aka ""Win32k OTF Validation Vulnerability."""  
  
[CVE-2011-1874] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1875] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1876] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1877] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1878] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1879] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1880] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1881] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1882] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1883] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1884] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-1885] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1886] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 does not properly validate the arguments to functions, which allows local users to read arbitrary data from kernel memory via a crafted application that triggers a NULL pointer dereference, aka ""Win32k Incorrect Parameter Validation Allows Information Disclosure Vulnerability."""  
  
[CVE-2011-1887] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1888] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1891] "Cross-site scripting (XSS) vulnerability in Microsoft Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters in a request to a script, aka ""Contact Details Reflected XSS Vulnerability."""  
  
[CVE-2011-1892] "Microsoft Office Groove 2007 SP2, SharePoint Workspace 2010 Gold and SP1, Office Forms Server 2007 SP2, Office SharePoint Server 2007 SP2, Office SharePoint Server 2010 Gold and SP1, Office Groove Data Bridge Server 2007 SP2, Office Groove Management Server 2007 SP2, Groove Server 2010 Gold and SP1, Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010, and Office Web Apps 2010 Gold and SP1 do not properly handle Web Parts containing XML classes referencing external entities, which allows remote authenticated users to read arbitrary files via a crafted XML and XSL file, aka ""SharePoint Remote File Disclosure Vulnerability."""  
  
[CVE-2011-1893] "Cross-site scripting (XSS) vulnerability in Microsoft Office SharePoint Server 2010, Windows SharePoint Services 2.0 and 3.0 SP2, and SharePoint Foundation 2010 allows remote attackers to inject arbitrary web script or HTML via the URI, aka ""SharePoint XSS Vulnerability."""  
  
[CVE-2011-1894] "The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for embedded content in an HTML document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted EMBED element in a web page that is visited in Internet Explorer, aka ""MHTML Mime-Formatted Request Vulnerability."""  
  
[CVE-2011-1965] "Tcpip.sys in the TCP/IP stack in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 does not properly implement URL-based QoS, which allows remote attackers to cause a denial of service (reboot) via a crafted URL to a web server, aka ""TCP/IP QOS Denial of Service Vulnerability."""  
  
[CVE-2011-1966] "The DNS server in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 does not properly handle NAPTR queries that trigger recursive processing, which allows remote attackers to execute arbitrary code via a crafted query, aka ""DNS NAPTR Query Vulnerability."""  
  
[CVE-2011-1967] "Winsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka ""CSRSS Vulnerability."""  
  
[CVE-2011-1968] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly process packets in memory, which allows remote attackers to cause a denial of service (reboot) by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, as exploited in the wild in 2011, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2011-1970] "The DNS server in Microsoft Windows Server 2003 SP2 and Windows Server 2008 SP2, R2, and R2 SP1 does not properly initialize memory, which allows remote attackers to cause a denial of service (service outage) via a query for a nonexistent domain, aka ""DNS Uninitialized Memory Corruption Vulnerability."""  
  
[CVE-2011-1971] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly parse file metadata, which allows local users to cause a denial of service (reboot) via a crafted file, aka ""Windows Kernel Metadata Parsing DOS Vulnerability."""  
  
[CVE-2011-1974] "NDISTAPI.sys in the NDISTAPI driver in Remote Access Service (RAS) in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka ""NDISTAPI Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1975] "Untrusted search path vulnerability in the Data Access Tracing component in Windows Data Access Components (Windows DAC) 6.0 in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an Excel .xlsx file, aka ""Data Access Components Insecure Library Loading Vulnerability."""  
  
[CVE-2011-1984] "WINS in Microsoft Windows Server 2003 SP2 and Server 2008 SP2, R2, and R2 SP1 allows local users to gain privileges by sending crafted packets over the loopback interface, aka ""WINS Local Elevation of Privilege Vulnerability."""  
  
[CVE-2011-1985] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka ""Win32k Null Pointer De-reference Vulnerability."""  
  
[CVE-2011-1991] "Multiple untrusted search path vulnerabilities in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .doc, .rtf, or .txt file, related to (1) deskpan.dll in the Display Panning CPL Extension, (2) EAPHost Authenticator Service, (3) Folder Redirection, (4) HyperTerminal, (5) the Japanese Input Method Editor (IME), and (6) Microsoft Management Console (MMC), aka ""Windows Components Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2002] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle TrueType fonts, which allows local users to cause a denial of service (system hang) via a crafted font file, aka ""Win32k TrueType Font Type Translation Vulnerability."""  
  
[CVE-2011-2003] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .fon file, aka ""Font Library File Buffer Overrun Vulnerability."""  
  
[CVE-2011-2004] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a crafted TrueType font file, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2011-3402."  
  
[CVE-2011-2005] "afd.sys in the Ancillary Function Driver in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2011-2009] "Untrusted search path vulnerability in Windows Media Center in Microsoft Windows Vista SP2 and Windows 7 Gold and SP1, and Windows Media Center TV Pack for Windows Vista, allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Media Center Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2011] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2011-2013] "Integer overflow in the TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code by sending a sequence of crafted UDP packets to a closed port, aka ""Reference Counter Overflow Vulnerability."""  
  
[CVE-2011-2014] "The LDAP over SSL (aka LDAPS) implementation in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not examine Certificate Revocation Lists (CRLs), which allows remote authenticated users to bypass intended certificate restrictions and access Active Directory resources by leveraging a revoked X.509 certificate for a domain account, aka ""LDAPS Authentication Bypass Vulnerability."""  
  
[CVE-2011-2016] "Untrusted search path vulnerability in Windows Mail and Windows Meeting Space in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .eml or .wcinv file, aka ""Windows Mail Insecure Library Loading Vulnerability."""  
  
[CVE-2011-2018] "The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 Gold and SP1 does not properly initialize objects, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Exception Handler Vulnerability."""  
  
[CVE-2011-2019] "Untrusted search path vulnerability in Microsoft Internet Explorer 9 on Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains an HTML file, aka ""Internet Explorer Insecure Library Loading Vulnerability."""  
  
[CVE-2011-3389] "The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a ""BEAST"" attack."  
  
[CVE-2011-3397] "The Microsoft Time component in DATIME.DLL in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted web site that leverages an unspecified ""binary behavior"" in Internet Explorer, aka ""Microsoft Time Remote Code Execution Vulnerability."""  
  
[CVE-2011-3400] "Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 do not properly handle OLE objects in memory, which allows remote attackers to execute arbitrary code via a crafted object in a file, aka ""OLE Property Vulnerability."""  
  
[CVE-2011-3401] "ENCDEC.DLL in Windows Media Player and Media Center in Microsoft Windows XP SP2 and SP3, Windows Vista SP2, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted .dvr-ms file, aka ""Windows Media Player DVR-MS Memory Corruption Vulnerability."""  
  
[CVE-2011-3402] "Unspecified vulnerability in the TrueType font parsing engine in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via crafted font data in a Word document or web page, as exploited in the wild in November 2011 by Duqu, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2011-3406] "Buffer overflow in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote authenticated users to execute arbitrary code via a crafted query that leverages incorrect memory initialization, aka ""Active Directory Buffer Overflow Vulnerability."""  
  
[CVE-2011-3408] "Csrsrv.dll in the Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly check permissions for sending inter-process device-event messages from low-integrity processes to high-integrity processes, which allows local users to gain privileges via a crafted application, aka ""CSRSS Local Privilege Elevation Vulnerability."""  
  
[CVE-2011-4434] Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 do not properly enforce AppLocker rules, which allows local users to bypass intended access restrictions via a (1) macro or (2) scripting feature in an application, as demonstrated by Microsoft Office applications and the SANDBOX\_INERT and LOAD\_IGNORE\_CODE\_AUTHZ\_LEVEL flags.  
  
[CVE-2011-4695] Unspecified vulnerability in Microsoft Windows 7 SP1, when Java is installed, allows local users to bypass Internet Explorer sandbox restrictions and gain privileges via unknown vectors, as demonstrated by the White Phosphorus wp\_ie\_sandbox\_escape module for Immunity CANVAS. NOTE: as of 20111207, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.  
  
[CVE-2011-5046] "The Graphics Device Interface (GDI) in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted data, as demonstrated by a large height attribute of an IFRAME element rendered by Safari, aka ""GDI Access Violation Vulnerability."""  
  
[CVE-2011-5279] CRLF injection vulnerability in the CGI implementation in Microsoft Internet Information Services (IIS) 4.x and 5.x on Windows NT and Windows 2000 allows remote attackers to modify arbitrary uppercase environment variables via a \n (newline) character in an HTTP header.  
  
[CVE-2012-0001] "The kernel in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly load structured exception handling tables, which allows context-dependent attackers to bypass the SafeSEH security feature by leveraging a Visual C++ .NET 2003 application, aka ""Windows Kernel SafeSEH Bypass Vulnerability."""  
  
[CVE-2012-0002] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2012-0003] "Unspecified vulnerability in winmm.dll in Windows Multimedia Library in Windows Media Player (WMP) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via a crafted MIDI file, aka ""MIDI Remote Code Execution Vulnerability."""  
  
[CVE-2012-0004] "Unspecified vulnerability in DirectShow in DirectX in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted media file, related to Quartz.dll, Qdvd.dll, closed captioning, and the Line21 DirectShow filter, aka ""DirectShow Remote Code Execution Vulnerability."""  
  
[CVE-2012-0005] "The Client/Server Run-time Subsystem (aka CSRSS) in the Win32 subsystem in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2, when a Chinese, Japanese, or Korean system locale is used, can access uninitialized memory during the processing of Unicode characters, which allows local users to gain privileges via a crafted application, aka ""CSRSS Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0006] "The DNS server in Microsoft Windows Server 2003 SP2 and Server 2008 SP2, R2, and R2 SP1 does not properly handle objects in memory during record lookup, which allows remote attackers to cause a denial of service (daemon restart) via a crafted query, aka ""DNS Denial of Service Vulnerability."""  
  
[CVE-2012-0009] "Untrusted search path vulnerability in the Windows Object Packager configuration in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse executable file in the current working directory, as demonstrated by a directory that contains a file with an embedded packaged object, aka ""Object Packager Insecure Executable Launching Vulnerability."""  
  
[CVE-2012-0013] "Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka ""Assembly Execution Vulnerability."""  
  
[CVE-2012-0148] "afd.sys in the Ancillary Function Driver in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 on 64-bit platforms does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""AfdPoll Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0149] "afd.sys in the Ancillary Function Driver in Microsoft Windows Server 2003 SP2 does not properly validate user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2012-0150] "Buffer overflow in msvcrt.dll in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted media file, aka ""Msvcrt.dll Buffer Overflow Vulnerability."""  
  
[CVE-2012-0151] "The Authenticode Signature Verification function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly validate the digest of a signed portable executable (PE) file, which allows user-assisted remote attackers to execute arbitrary code via a modified file with additional content, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2012-0152] "The Remote Desktop Protocol (RDP) service in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka ""Terminal Server Denial of Service Vulnerability."""  
  
[CVE-2012-0154] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers keyboard layout errors, aka ""Keyboard Layout Use After Free Vulnerability."""  
  
[CVE-2012-0156] "DirectWrite in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly render Unicode characters, which allows remote attackers to cause a denial of service (application hang) via a (1) instant message or (2) web site, aka ""DirectWrite Application Denial of Service Vulnerability."""  
  
[CVE-2012-0157] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle window messaging, which allows local users to gain privileges via a crafted application that calls the PostMessage function, aka ""PostMessage Function Vulnerability."""  
  
[CVE-2012-0159] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview  
[CVE-2012-0164] "Microsoft .NET Framework 4 does not properly compare index values, which allows remote attackers to cause a denial of service (application hang) via crafted requests to a Windows Presentation Foundation (WPF) application, aka "".NET Framework Index Comparison Vulnerability."""  
  
[CVE-2012-0165] "GDI+ in Microsoft Windows Vista SP2 and Server 2008 SP2 and Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1 does not properly validate record types in EMF images, which allows remote attackers to execute arbitrary code via a crafted image, aka ""GDI+ Record Type Vulnerability."""  
  
[CVE-2012-0173] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka ""Remote Desktop Protocol Vulnerability,"" a different vulnerability than CVE-2012-0002."  
  
[CVE-2012-0174] "Windows Firewall in tcpip.sys in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly enforce firewall rules for outbound broadcast packets, which allows remote attackers to obtain potentially sensitive information by observing broadcast traffic on a local network, aka ""Windows Firewall Bypass Vulnerability."""  
  
[CVE-2012-0175] "The Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted name for a (1) file or (2) directory, aka ""Command Injection Vulnerability."""  
  
[CVE-2012-0176] "Double free vulnerability in Microsoft Silverlight 4 before 4.1.10329 on Windows allows remote attackers to execute arbitrary code via vectors involving crafted XAML glyphs, aka ""Silverlight Double-Free Vulnerability."""  
  
[CVE-2012-0178] "Race condition in partmgr.sys in Windows Partition Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that makes multiple simultaneous Plug and Play (PnP) Configuration Manager function calls, aka ""Plug and Play (PnP) Configuration Manager Vulnerability."""  
  
[CVE-2012-0179] "Double free vulnerability in tcpip.sys in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that binds an IPv6 address to a local interface, aka ""TCP/IP Double Free Vulnerability."""  
  
[CVE-2012-0180] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly handle user-mode input passed to kernel mode for (1) windows and (2) messages, which allows local users to gain privileges via a crafted application, aka ""Windows and Messages Vulnerability."""  
  
[CVE-2012-0181] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly manage Keyboard Layout files, which allows local users to gain privileges via a crafted application, aka ""Keyboard Layout File Vulnerability."""  
  
[CVE-2012-1194] "The resolver in the DNS Server service in Microsoft Windows Server 2008 before R2 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a ""ghost domain names"" attack."  
  
[CVE-2012-1527] "Integer underflow in Windows Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows local users to gain privileges via a crafted briefcase, aka ""Windows Briefcase Integer Underflow Vulnerability."""  
  
[CVE-2012-1528] "Integer overflow in Windows Shell in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows local users to gain privileges via a crafted briefcase, aka ""Windows Briefcase Integer Overflow Vulnerability."""  
  
[CVE-2012-1537] "Heap-based buffer overflow in DirectPlay in DirectX 9.0 through 11.1 in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a crafted Office document, aka ""DirectPlay Heap Overflow Vulnerability."""  
  
[CVE-2012-1848] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and Windows 8 Consumer Preview does not properly handle user-mode input passed to kernel mode, which allows local users to gain privileges via a crafted application, aka ""Scrollbar Calculation Vulnerability."""  
  
[CVE-2012-1850] "The Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle RAP responses, which allows remote attackers to cause a denial of service (service hang) via crafted RAP packets, aka ""Remote Administration Protocol Denial of Service Vulnerability."""  
  
[CVE-2012-1851] "Format string vulnerability in the Print Spooler service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted response, aka ""Print Spooler Service Format String Vulnerability."""  
  
[CVE-2012-1852] "Heap-based buffer overflow in the Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP2 and SP3 allows remote attackers to execute arbitrary code via crafted RAP response packets, aka ""Remote Administration Protocol Heap Overflow Vulnerability."""  
  
[CVE-2012-1853] "Stack-based buffer overflow in the Remote Administration Protocol (RAP) implementation in the LanmanWorkstation service in Microsoft Windows XP SP3 allows remote attackers to execute arbitrary code via crafted RAP response packets, aka ""Remote Administration Protocol Stack Overflow Vulnerability."""  
  
[CVE-2012-1863] "Cross-site scripting (XSS) vulnerability in Microsoft Office SharePoint Server 2007 SP2 and SP3 Windows SharePoint Services 3.0 SP2, and SharePoint Foundation 2010 Gold and SP1 allows remote attackers to inject arbitrary web script or HTML via crafted JavaScript elements in a URL, aka ""SharePoint Reflected List Parameter Vulnerability."""  
  
[CVE-2012-1864] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""String Atom Class Name Handling Vulnerability,"" a different vulnerability than CVE-2012-1865."  
  
[CVE-2012-1865] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""String Atom Class Name Handling Vulnerability,"" a different vulnerability than CVE-2012-1864."  
  
[CVE-2012-1866] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle user-mode input passed to kernel mode for driver objects, which allows local users to gain privileges via a crafted application, aka ""Clipboard Format Atom Name Handling Vulnerability."""  
  
[CVE-2012-1867] "Integer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted TrueType font file that triggers incorrect memory allocation, aka ""Font Resource Refcount Integer Overflow Vulnerability."""  
  
[CVE-2012-1868] "Race condition in the thread-creation implementation in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3 allows local users to gain privileges via a crafted application, aka ""Win32k.sys Race Condition Vulnerability."""  
  
[CVE-2012-1870] "The CBC mode in the TLS protocol, as used in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, and other products, allows remote web servers to obtain plaintext data by triggering multiple requests to a third-party HTTPS server and sniffing the network during the resulting HTTPS session, aka ""TLS Protocol Vulnerability."""  
  
[CVE-2012-1890] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle keyboard-layout files, which allows local users to gain privileges via a crafted application, aka ""Keyboard Layout Vulnerability."""  
  
[CVE-2012-1891] "Heap-based buffer overflow in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2 and Windows Data Access Components (WDAC) 6.0 allows remote attackers to execute arbitrary code via crafted XML data that triggers access to an uninitialized object in memory, aka ""ADO Cachesize Heap Overflow RCE Vulnerability."""  
  
[CVE-2012-1893] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate callback parameters during creation of a hook procedure, which allows local users to gain privileges via a crafted application, aka ""Win32k Incorrect Type Handling Vulnerability."""  
  
[CVE-2012-1945] Mozilla Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10 allow local users to obtain sensitive information via an HTML document that loads a shortcut (aka .lnk) file for display within an IFRAME element, as demonstrated by a network share implemented by (1) Microsoft Windows or (2) Samba.  
  
[CVE-2012-2520] "Cross-site scripting (XSS) vulnerability in Microsoft InfoPath 2007 SP2 and SP3 and 2010 SP1, Communicator 2007 R2, Lync 2010 and 2010 Attendee, SharePoint Server 2007 SP2 and SP3 and 2010 SP1, Groove Server 2010 SP1, Windows SharePoint Services 3.0 SP2, SharePoint Foundation 2010 SP1, and Office Web Apps 2010 SP1 allows remote attackers to inject arbitrary web script or HTML via a crafted string, aka ""HTML Sanitization Vulnerability."""  
  
[CVE-2012-2526] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP3 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to a deleted object, aka ""Remote Desktop Protocol Vulnerability."""  
  
[CVE-2012-2527] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2529] "Integer overflow in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Windows Kernel Integer Overflow Vulnerability."""  
  
[CVE-2012-2530] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2551] "The server in Kerberos in Microsoft Windows Server 2008 R2 and R2 SP1, and Windows 7 Gold and SP1, allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via a crafted session request, aka ""Kerberos NULL Dereference Vulnerability."""  
  
[CVE-2012-2553] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2012-2556] "The OpenType Font (OTF) driver in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to execute arbitrary code via a crafted OpenType font file, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2012-2897] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT, as used by Google Chrome before 22.0.1229.79 and other programs, do not properly handle objects in memory, which allows remote attackers to execute arbitrary code via a crafted TrueType font file, aka ""Windows Font Parsing Vulnerability"" or ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2012-2971] The server in CA ARCserve Backup r12.5, r15, and r16 on Windows does not properly process RPC requests, which allows remote attackers to execute arbitrary code or cause a denial of service via a crafted request.  
  
[CVE-2012-2972] The (1) server and (2) agent components in CA ARCserve Backup r12.5, r15, and r16 on Windows do not properly validate RPC requests, which allows remote attackers to cause a denial of service (service crash) via a crafted request.  
  
[CVE-2012-2993] Microsoft Windows Phone 7 does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof an SSL server for the (1) POP3, (2) IMAP, or (3) SMTP protocol via an arbitrary valid certificate.  
  
[CVE-2012-4774] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allow remote attackers to execute arbitrary code via a crafted (1) file name or (2) subfolder name that triggers use of unallocated memory as the destination of a copy operation, aka ""Windows Filename Parsing Vulnerability."""  
  
[CVE-2012-4786] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a crafted TrueType Font (TTF) file, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2012-5362] The IPv6 implementation in Microsoft Windows 7 and earlier allows remote attackers to cause a denial of service via a flood of ICMPv6 Neighbor Solicitation messages, a different vulnerability than CVE-2010-4669.  
  
[CVE-2012-5364] The IPv6 implementation in Microsoft Windows 7 and earlier allows remote attackers to cause a denial of service via a flood of ICMPv6 Router Advertisement packets containing multiple Routing entries.  
  
[CVE-2013-0001] "The Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 4, and 4.5 does not properly initialize memory arrays, which allows remote attackers to obtain sensitive information via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application that leverages a pointer to an unmanaged memory location, aka ""System Drawing Information Disclosure Vulnerability."""  
  
[CVE-2013-0002] "Buffer overflow in the Windows Forms (aka WinForms) component in Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4, and 4.5 allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application that leverages improper counting of objects during a memory copy operation, aka ""WinForms Buffer Overflow Vulnerability."""  
  
[CVE-2013-0005] "The WCF Replace function in the Open Data (aka OData) protocol implementation in Microsoft .NET Framework 3.5, 3.5 SP1, 3.5.1, and 4, and the Management OData IIS Extension on Windows Server 2012, allows remote attackers to cause a denial of service (resource consumption and daemon restart) via crafted values in HTTP requests, aka ""Replace Denial of Service Vulnerability."""  
  
[CVE-2013-0008] "win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle window broadcast messages, which allows local users to gain privileges via a crafted application, aka ""Win32k Improper Message Handling Vulnerability."""  
  
[CVE-2013-0011] "The Print Spooler in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted print job, aka ""Windows Print Spooler Components Vulnerability."""  
  
[CVE-2013-0013] "The SSL provider component in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle encrypted packets, which allows man-in-the-middle attackers to conduct SSLv2 downgrade attacks against (1) SSLv3 sessions or (2) TLS sessions by intercepting handshakes and injecting content, aka ""Microsoft SSL Version 3 and TLS Protocol Security Feature Bypass Vulnerability."""  
  
[CVE-2013-0073] "The Windows Forms (aka WinForms) component in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, and 4.5 does not properly restrict the privileges of a callback function during object creation, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (XBAP) or (2) a crafted .NET Framework application, aka ""WinForms Callback Elevation Vulnerability."""  
  
[CVE-2013-0075] "The TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (reboot) via a crafted packet that terminates a TCP connection, aka ""TCP FIN WAIT Vulnerability."""  
  
[CVE-2013-0076] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Reference Count Vulnerability."""  
  
[CVE-2013-0077] "Quartz.dll in DirectShow in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows remote attackers to execute arbitrary code via crafted media content in (1) a media file, (2) a media stream, or (3) a Microsoft Office document, aka ""Media Decompression Vulnerability."""  
  
[CVE-2013-0078] "The Microsoft Antimalware Client in Windows Defender on Windows 8 and Windows RT uses an incorrect pathname for MsMpEng.exe, which allows local users to gain privileges via a crafted application, aka ""Microsoft Antimalware Improper Pathname Vulnerability."""  
  
[CVE-2013-0096] "Writer in Microsoft Windows Essentials 2011 and 2012 allows remote attackers to bypass proxy settings and overwrite arbitrary files via crafted URL parameters, aka ""Windows Essentials Improper URI Handling Vulnerability."""  
  
[CVE-2013-0810] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, and Windows Server 2008 SP2 allow remote attackers to execute arbitrary code via a crafted screensaver in a theme file, aka ""Windows Theme File Remote Code Execution Vulnerability."""  
  
[CVE-2013-0941] EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.  
  
[CVE-2013-1248] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1249] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1250] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1251] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1252] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1253] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1254] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1255] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1256] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1257] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1258] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1259] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1260] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1261] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1262] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1263] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1264] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1265] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1266] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1267] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1268] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1269] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1270] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1271] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1272] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1273] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1274] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1275] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1276] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1277] Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges, and consequently read the contents of arbitrary kernel memory locations, via a crafted application, a different vulnerability than other CVEs listed in MS13-016.  
  
[CVE-2013-1278] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages incorrect handling of objects in memory, aka ""Kernel Race Condition Vulnerability,"" a different vulnerability than CVE-2013-1279."  
  
[CVE-2013-1279] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages incorrect handling of objects in memory, aka ""Kernel Race Condition Vulnerability,"" a different vulnerability than CVE-2013-1278."  
  
[CVE-2013-1280] "The kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Reference Count Vulnerability."""  
  
[CVE-2013-1281] "The NFS server in Microsoft Windows Server 2008 R2 and R2 SP1 and Server 2012 allows remote attackers to cause a denial of service (NULL pointer dereference and reboot) via an attempted renaming of a file or folder located on a read-only share, aka ""NULL Dereference Vulnerability."""  
  
[CVE-2013-1283] "Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Race Condition Vulnerability."""  
  
[CVE-2013-1284] "Race condition in the kernel in Microsoft Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Kernel Race Condition Vulnerability."""  
  
[CVE-2013-1285] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1286 and CVE-2013-1287."  
  
[CVE-2013-1286] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1285 and CVE-2013-1287."  
  
[CVE-2013-1287] "The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability,"" a different vulnerability than CVE-2013-1285 and CVE-2013-1286."  
  
[CVE-2013-1291] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 Gold and SP1, and Windows 8 allows local users to cause a denial of service (reboot) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability"" or ""Win32k Font Parsing Vulnerability."""  
  
[CVE-2013-1292] "Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Race Condition Vulnerability."""  
  
[CVE-2013-1293] "The NTFS kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application that leverages improper handling of objects in memory, aka ""NTFS NULL Pointer Dereference Vulnerability."""  
  
[CVE-2013-1294] "Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Kernel Race Condition Vulnerability."""  
  
[CVE-2013-1295] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP2, and Server 2008 SP2 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""CSRSS Memory Corruption Vulnerability."""  
  
[CVE-2013-1299] Microsoft Windows Modern Mail allows remote attackers to spoof link targets via a crafted HTML e-mail message.  
  
[CVE-2013-1300] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Allocation Vulnerability."""  
  
[CVE-2013-1305] "HTTP.sys in Microsoft Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (infinite loop) via a crafted HTTP header, aka ""HTTP.sys Denial of Service Vulnerability."""  
  
[CVE-2013-1313] "Object Linking and Embedding (OLE) Automation in Microsoft Windows XP SP3 does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted RTF document, aka ""OLE Automation Remote Code Execution Vulnerability."""  
  
[CVE-2013-1332] "dxgkrnl.sys (aka the DirectX graphics kernel subsystem) in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""DirectX Graphics Kernel Subsystem Double Fetch Vulnerability."""  
  
[CVE-2013-1333] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2013-1334] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Handle Vulnerability."""  
  
[CVE-2013-1337] "Microsoft .NET Framework 4.5 does not properly create policy requirements for custom Windows Communication Foundation (WCF) endpoint authentication in certain situations involving passwords over HTTPS, which allows remote attackers to bypass authentication by sending queries to an endpoint, aka ""Authentication Bypass Vulnerability."""  
  
[CVE-2013-1339] "The Print Spooler in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly manage memory during deletion of printer connections, which allows remote authenticated users to execute arbitrary code via a crafted request, aka ""Print Spooler Vulnerability."""  
  
[CVE-2013-1340] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Dereference Vulnerability."""  
  
[CVE-2013-1341] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 8 allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability."""  
  
[CVE-2013-1342] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1343] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1344, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1344] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-3864, and CVE-2013-3865."  
  
[CVE-2013-1345] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Vulnerability."""  
  
[CVE-2013-2552] Unspecified vulnerability in Microsoft Internet Explorer 10 on Windows 8 allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a Medium integrity process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.  
  
[CVE-2013-2553] Unspecified vulnerability in the kernel in Microsoft Windows 7 allows local users to gain privileges via unknown vectors, as demonstrated by Nils and Jon of MWR Labs during a Pwn2Own competition at CanSecWest 2013, a different vulnerability than CVE-2013-0912.  
  
[CVE-2013-2554] Unspecified vulnerability in Microsoft Windows 7 allows attackers to bypass the ASLR and DEP protection mechanisms via unknown vectors, as demonstrated against Firefox by VUPEN during a Pwn2Own competition at CanSecWest 2013, a different vulnerability than CVE-2013-0787.  
  
[CVE-2013-2556] "Unspecified vulnerability in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 through SP1 allows attackers to bypass the ASLR protection mechanism via unknown vectors, as demonstrated against Adobe Flash Player by VUPEN during a Pwn2Own competition at CanSecWest 2013, aka ""ASLR Security Feature Bypass Vulnerability."""  
  
[CVE-2013-2558] Unspecified vulnerability in Microsoft Windows 8 allows remote attackers to cause a denial of service (reboot) or possibly have unknown other impact via a crafted TrueType Font (TTF) file, as demonstrated by the 120612-69701-01.dmp error report.  
  
[CVE-2013-3127] "The Microsoft WMV video codec in wmv9vcm.dll, wmvdmod.dll in Windows Media Format Runtime 9 and 9.5, and wmvdecod.dll in Windows Media Format Runtime 11 and Windows Media Player 11 and 12 allows remote attackers to execute arbitrary code via a crafted media file, aka ""WMV Video Decoder Remote Code Execution Vulnerability."""  
  
[CVE-2013-3128] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, and 4.5, allow remote attackers to execute arbitrary code via a crafted OpenType font (OTF) file, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2013-3136] "The kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly handle unspecified page-fault system calls, which allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Kernel Information Disclosure Vulnerability."""  
  
[CVE-2013-3138] "Integer overflow in the TCP/IP kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to cause a denial of service (system hang) via crafted TCP packets, aka ""TCP/IP Integer Overflow Vulnerability."""  
  
[CVE-2013-3154] "The signature-update functionality in Windows Defender on Microsoft Windows 7 and Windows Server 2008 R2 relies on an incorrect pathname, which allows local users to gain privileges via a Trojan horse application in the %SYSTEMDRIVE% top-level directory, aka ""Microsoft Windows 7 Defender Improper Pathname Vulnerability."""  
  
[CVE-2013-3167] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2013-3172] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to cause a denial of service (system hang) via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2013-3173] "Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that leverages improper handling of objects in memory, aka ""Win32k Buffer Overwrite Vulnerability."""  
  
[CVE-2013-3174] "DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a crafted GIF file, aka ""DirectShow Arbitrary Memory Overwrite Vulnerability."""  
  
[CVE-2013-3181] "usp10.dll in the Unicode Scripts Processor in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""Uniscribe Font Parsing Engine Memory Corruption Vulnerability."""  
  
[CVE-2013-3182] "The Windows NAT Driver (aka winnat) service in Microsoft Windows Server 2012 does not properly validate memory addresses during the processing of ICMP packets, which allows remote attackers to cause a denial of service (memory corruption and system hang) via crafted packets, aka ""Windows NAT Denial of Service Vulnerability."""  
  
[CVE-2013-3183] "The TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly perform memory allocation for inbound ICMPv6 packets, which allows remote attackers to cause a denial of service (system hang) via crafted packets, aka ""ICMPv6 Vulnerability."""  
  
[CVE-2013-3185] "Microsoft Active Directory Federation Services (AD FS) 1.x through 2.1 on Windows Server 2003 R2 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 allows remote attackers to obtain sensitive information about the service account, and possibly conduct account-lockout attacks, by connecting to an endpoint, aka ""AD FS Information Disclosure Vulnerability."""  
  
[CVE-2013-3186] "The Protected Mode feature in Microsoft Internet Explorer 7 through 10 on Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly implement the Integrity Access Level (aka IL) protection mechanism, which allows remote attackers to obtain medium-integrity privileges by leveraging access to a low-integrity process, aka ""Process Integrity Level Assignment Vulnerability."""  
  
[CVE-2013-3195] "The DSA\_InsertItem function in Comctl32.dll in the Windows common control library in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted value in an argument to an ASP.NET web application, aka ""Comctl32 Integer Overflow Vulnerability."""  
  
[CVE-2013-3196] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3197 and CVE-2013-3198."  
  
[CVE-2013-3197] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3196 and CVE-2013-3198."  
  
[CVE-2013-3198] "The NT Virtual DOS Machine (NTVDM) subsystem in the kernel in Microsoft Windows XP SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 on 32-bit platforms does not properly validate kernel-memory addresses, which allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability,"" a different vulnerability than CVE-2013-3196 and CVE-2013-3197."  
  
[CVE-2013-3200] "The USB drivers in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Windows USB Descriptor Vulnerability."""  
  
[CVE-2013-3660] "The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 does not properly initialize a pointer for the next object in a certain list, which allows local users to obtain write access to the PATHRECORD chain, and consequently gain privileges, by triggering excessive consumption of paged memory and then making many FlattenPath function calls, aka ""Win32k Read AV Vulnerability."""  
  
[CVE-2013-3661] The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not check whether linked-list traversal is continually accessing the same list member, which allows local users to cause a denial of service (infinite traversal) via vectors that trigger a crafted PATHRECORD chain.  
  
[CVE-2013-3862] "Double free vulnerability in Microsoft Windows 7 and Server 2008 R2 SP1 allows local users to gain privileges via a crafted service description that is not properly handled by services.exe in the Service Control Manager (SCM), aka ""Service Control Manager Double Free Vulnerability."""  
  
[CVE-2013-3863] "Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allow remote attackers to execute arbitrary code via a crafted OLE object in a file, aka ""OLE Property Vulnerability."""  
  
[CVE-2013-3864] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, and CVE-2013-3865."  
  
[CVE-2013-3865] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Multiple Fetch Vulnerability,"" a different vulnerability than CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, and CVE-2013-3864."  
  
[CVE-2013-3866] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2013-3868] "Microsoft Active Directory Lightweight Directory Service (AD LDS) on Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 8 and Active Directory Services on Windows Server 2008 SP2 and R2 SP1 and Server 2012 allow remote attackers to cause a denial of service (LDAP directory-service outage) via a crafted LDAP query, aka ""Remote Anonymous DoS Vulnerability."""  
  
[CVE-2013-3869] "Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to cause a denial of service (daemon hang) via a web-service request containing a crafted X.509 certificate that is not properly handled during validation, aka ""Digital Signatures Vulnerability."""  
  
[CVE-2013-3876] DirectAccess in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly verify server X.509 certificates, which allows man-in-the-middle attackers to spoof servers and read encrypted domain credentials via a crafted certificate.  
  
[CVE-2013-3879] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2013-3880] "The App Container feature in the kernel-mode drivers in Microsoft Windows 8, Windows Server 2012, and Windows RT allows remote attackers to bypass intended access restrictions and obtain sensitive information from a different container via a Trojan horse application, aka ""App Container Elevation of Privilege Vulnerability."""  
  
[CVE-2013-3881] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges via a crafted application, aka ""Win32k NULL Page Vulnerability."""  
  
[CVE-2013-3887] "The Ancillary Function Driver (AFD) in afd.sys in the kernel-mode drivers in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 allows local users to obtain sensitive information from kernel memory by leveraging improper copy operations, aka ""Ancillary Function Driver Information Disclosure Vulnerability."""  
  
[CVE-2013-3888] "dxgkrnl.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""DirectX Graphics Kernel Subsystem Double Fetch Vulnerability."""  
  
[CVE-2013-3894] "The kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allow remote attackers to execute arbitrary code via a crafted CMAP table in a TrueType font (TTF) file, aka ""TrueType Font CMAP Table Vulnerability."""  
  
[CVE-2013-3898] "Microsoft Windows 8 and Windows Server 2012, when Hyper-V is used, does not ensure memory-address validity, which allows guest OS users to execute arbitrary code in all guest OS instances, and allows guest OS users to cause a denial of service (host OS crash), via a guest-to-host hypercall with a crafted function parameter, aka ""Address Corruption Vulnerability."""  
  
[CVE-2013-3899] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly validate addresses, which allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Vulnerability."""  
  
[CVE-2013-3900] "The WinVerifyTrust function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate PE file digests during Authenticode signature verification, which allows remote attackers to execute arbitrary code via a crafted PE file, aka ""WinVerifyTrust Signature Validation Vulnerability."""  
  
[CVE-2013-3902] "Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1 and Windows 7 SP1 on 64-bit platforms allows local users to gain privileges via a crafted application, aka ""Win32k Use After Free Vulnerability."""  
  
[CVE-2013-3903] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to cause a denial of service (reboot) via a crafted TrueType font (TTF) file, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2013-3906] "GDI+ in Microsoft Windows Vista SP2 and Server 2008 SP2  
[CVE-2013-3907] "portcls.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Port-Class Driver Double Fetch Vulnerability."""  
  
[CVE-2013-3918] "The InformationCardSigninHelper Class ActiveX control in icardie.dll in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted web page that is accessed by Internet Explorer, as exploited in the wild in November 2013, aka ""InformationCardSigninHelper Vulnerability."""  
  
[CVE-2013-3940] "Integer overflow in the Graphics Device Interface (GDI) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image in a Windows Write (.wri) document, which is not properly handled in WordPad, aka ""Graphics Device Interface Integer Overflow Vulnerability."""  
  
[CVE-2013-4858] Microsoft Windows Movie Maker 2.1.4026.0 on Windows XP SP3 allows remote attackers to cause a denial of service (application crash) via a crafted .wav file, as demonstrated by movieMaker.wav.  
  
[CVE-2013-5056] "Use-after-free vulnerability in the Scripting Runtime Object Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site that is visited with Internet Explorer, aka ""Use-After-Free Vulnerability in Microsoft Scripting Runtime Object Library."""  
  
[CVE-2013-5058] "Integer overflow in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows local users to gain privileges via a crafted application, aka ""Win32k Integer Overflow Vulnerability."""  
  
[CVE-2013-5065] NDProxy.sys in the kernel in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a crafted application, as exploited in the wild in November 2013.  
  
[CVE-2013-6230] The Winsock WSAIoctl API in Microsoft Windows Server 2008, as used in ISC BIND 9.6-ESV before 9.6-ESV-R10-P1, 9.8 before 9.8.6-P1, 9.9 before 9.9.4-P1, 9.9.3-S1, 9.9.4-S1, and other products, does not properly support the SIO\_GET\_INTERFACE\_LIST command for netmask 255.255.255.255, which allows remote attackers to bypass intended IP address restrictions by leveraging misinterpretation of this netmask as a 0.0.0.0 netmask.  
  
[CVE-2013-6801] "Microsoft Word 2003 SP2 and SP3 on Windows XP SP3 allows remote attackers to cause a denial of service (CPU consumption) via a malformed .doc file containing an embedded image, as demonstrated by word2003forkbomb.doc, related to a ""fork bomb"" issue."  
  
[CVE-2013-6999] "\*\* DISPUTED \*\* The IsHandleEntrySecure function in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 SP2 does not properly validate the tagPROCESSINFO pW32Job field, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted NtUserValidateHandleSecure call for an owned object. NOTE: the vendor reportedly disputes the significance of this report, stating that ""it appears to be a local DOS ... we don't consider it a security vulnerability."""  
  
[CVE-2013-7331] The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers to determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes, as demonstrated by a res:// URL, and exploited in the wild in February 2014.  
  
[CVE-2013-7332] The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier does not properly detect recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.  
  
[CVE-2013-7369] SQL injection vulnerability in an unspecified DLL in the FSDBCom ActiveX control in F-Secure Anti-Virus for Microsoft Exchange Server before HF02, Anti-Virus for Windows Servers 9.00 before HF09, Anti-Virus for Citrix Servers 9.00 before HF09, and F-Secure Email and Server Security and F-Secure Server Security 9.20 before HF01 allows remote attackers to execute arbitrary SQL commands via unknown vectors, related to GetCommand.  
  
[CVE-2014-0251] "Microsoft Windows SharePoint Services 3.0 SP3  
[CVE-2014-0254] "The IPv6 implementation in Microsoft Windows 8, Windows Server 2012, and Windows RT does not properly validate packets, which allows remote attackers to cause a denial of service (system hang) via crafted ICMPv6 Router Advertisement packets, aka ""TCP/IP Version 6 (IPv6) Denial of Service Vulnerability."""  
  
[CVE-2014-0255] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka ""iSCSI Target Remote Denial of Service Vulnerability."""  
  
[CVE-2014-0256] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka ""iSCSI Target Remote Denial of Service Vulnerability."""  
  
[CVE-2014-0262] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1 and Server 2008 R2 SP1 does not properly consider thread-owned objects during the processing of window handles, which allows local users to gain privileges via a crafted application, aka ""Win32k Window Handle Vulnerability."""  
  
[CVE-2014-0263] "The Direct2D implementation in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a large 2D geometric figure that is encountered with Internet Explorer, aka ""Microsoft Graphics Component Memory Corruption Vulnerability."""  
  
[CVE-2014-0266] "The XMLHTTP ActiveX controls in XML Core Services 3.0 in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to bypass the Same Origin Policy via a web page that is visited in Internet Explorer, aka ""MSXML Information Disclosure Vulnerability."""  
  
[CVE-2014-0296] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly encrypt sessions, which makes it easier for man-in-the-middle attackers to obtain sensitive information by sniffing the network or modify session content by sending crafted RDP packets, aka ""RDP MAC Vulnerability."""  
  
[CVE-2014-0300] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2014-0301] "Double free vulnerability in qedit.dll in DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via a crafted JPEG image, aka ""DirectShow Memory Corruption Vulnerability."""  
  
[CVE-2014-0315] "Untrusted search path vulnerability in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a Trojan horse cmd.exe file in the current working directory, as demonstrated by a directory that contains a .bat or .cmd file, aka ""Windows File Handling Vulnerability."""  
  
[CVE-2014-0317] "The Security Account Manager Remote (SAMR) protocol implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2 does not properly determine the user-lockout state, which makes it easier for remote attackers to bypass the account lockout policy and obtain access via a brute-force attack, aka ""SAMR Security Feature Bypass Vulnerability."""  
  
[CVE-2014-0318] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly control access to thread-owned objects, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2014-0323] "win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (system hang) via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2014-1767] "Double free vulnerability in the Ancillary Function Driver (AFD) in afd.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Ancillary Function Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2014-1807] "The ShellExecute API in Windows Shell in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly implement file associations, which allows local users to gain privileges via a crafted application, as exploited in the wild in May 2014, aka ""Windows Shell File Association Vulnerability."""  
  
[CVE-2014-1811] "The TCP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (non-paged pool memory consumption and system hang) via malformed data in the Options field of a TCP header, aka ""TCP Denial of Service Vulnerability."""  
  
[CVE-2014-1812] "The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka ""Group Policy Preferences Password Elevation of Privilege Vulnerability."""  
  
[CVE-2014-1814] "The Windows Installer in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application that invokes the repair feature for a different application, aka ""Windows Installer Repair Vulnerability."""  
  
[CVE-2014-1817] "usp10.dll in Uniscribe (aka the Unicode Script Processor) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted EMF+ record in a font file, aka ""Unicode Scripts Processor Vulnerability."""  
  
[CVE-2014-1818] "GDI+ in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code via a crafted EMF+ record in an image file, aka ""GDI+ Image Parsing Vulnerability."""  
  
[CVE-2014-1819] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly control access to objects associated with font files, which allows local users to gain privileges via a crafted file, aka ""Font Double-Fetch Vulnerability."""  
  
[CVE-2014-1824] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted Journal (aka .JNT) file, aka ""Windows Journal Remote Code Execution Vulnerability."""  
  
[CVE-2014-2671] Microsoft Windows Media Player (WMP) 11.0.5721.5230 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted WAV file.  
  
[CVE-2014-2780] "DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows local users to gain privileges by leveraging control over a low-integrity process to execute a crafted application, aka ""DirectShow Elevation of Privilege Vulnerability."""  
  
[CVE-2014-2781] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly restrict the exchange of keyboard and mouse data between programs at different integrity levels, which allows attackers to bypass intended access restrictions by leveraging control over a low-integrity process to launch the On-Screen Keyboard (OSK) and then upload a crafted application, aka ""On-Screen Keyboard Elevation of Privilege Vulnerability."""  
  
[CVE-2014-2814] "Microsoft Service Bus 1.1 on Microsoft Windows Server 2008 R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (AMQP messaging outage) via crafted AMQP messages, aka ""Service Bus Denial of Service Vulnerability."""  
  
[CVE-2014-4060] "Use-after-free vulnerability in MCPlayer.dll in Microsoft Windows Media Center TV Pack for Windows Vista, Windows 7 SP1, and Windows Media Center for Windows 8 and 8.1 allows remote attackers to execute arbitrary code via a crafted Office document that triggers deletion of a CSyncBasePlayer object, aka ""CSyncBasePlayer Use After Free Vulnerability."""  
  
[CVE-2014-4064] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly handle use of the paged kernel pool for allocation of uninitialized memory, which allows local users to obtain sensitive information about kernel addresses via a crafted application, aka ""Windows Kernel Pool Allocation Vulnerability."""  
  
[CVE-2014-4074] "The Task Scheduler in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via an application that schedules a crafted task, aka ""Task Scheduler Vulnerability."""  
  
[CVE-2014-4076] "Microsoft Windows Server 2003 SP2 allows local users to gain privileges via a crafted IOCTL call to (1) tcpip.sys or (2) tcpip6.sys, aka ""TCP/IP Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4077] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Office 2007 SP3, when IMJPDCT.EXE (aka IME for Japanese) is installed, allow remote attackers to bypass a sandbox protection mechanism via a crafted PDF document, aka ""Microsoft IME (Japanese) Elevation of Privilege Vulnerability,"" as exploited in the wild in 2014."  
  
[CVE-2014-4113] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, as exploited in the wild in October 2014, aka ""Win32k.sys Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4114] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a ""Sandworm"" attack in June through October 2014, aka ""Windows OLE Remote Code Execution Vulnerability."""  
  
[CVE-2014-4115] "fastfat.sys (aka the FASTFAT driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 does not properly allocate memory, which allows physically proximate attackers to execute arbitrary code or cause a denial of service (reserved-memory write) by connecting a crafted USB device, aka ""Microsoft Windows Disk Partition Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2014-4118] "XML Core Services (aka MSXML) 3.0 in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (system-state corruption) via crafted XML content, aka ""MSXML Remote Code Execution Vulnerability."""  
  
[CVE-2014-4148] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted TrueType font, as exploited in the wild in October 2014, aka ""TrueType Font Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2014-4971] Microsoft Windows XP SP3 does not validate addresses in certain IRP handler routines, which allows local users to write data to arbitrary memory locations, and consequently gain privileges, via a crafted address in an IOCTL call, related to (1) the MQAC.sys driver in the MQ Access Control subsystem and (2) the BthPan.sys driver in the Bluetooth Personal Area Networking subsystem.  
  
[CVE-2014-6317] "Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (reboot) via a crafted TrueType font, aka ""Denial of Service in Windows Kernel Mode Driver Vulnerability."""  
  
[CVE-2014-6318] "The audit logon feature in Remote Desktop Protocol (RDP) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly log unauthorized login attempts supplying valid credentials, which makes it easier for remote attackers to bypass intended access restrictions via a series of attempts, aka ""Remote Desktop Protocol (RDP) Failure to Audit Vulnerability."""  
  
[CVE-2014-6321] "Schannel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via crafted packets, aka ""Microsoft Schannel Remote Code Execution Vulnerability."""  
  
[CVE-2014-6322] "The Windows Audio service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via a crafted web site, as demonstrated by execution of web script in Internet Explorer, aka ""Windows Audio Service Vulnerability."""  
  
[CVE-2014-6324] "The Kerberos Key Distribution Center (KDC) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote authenticated domain users to obtain domain administrator privileges via a forged signature in a ticket, as exploited in the wild in November 2014, aka ""Kerberos Checksum Vulnerability."""  
  
[CVE-2014-6332] "OleAut32.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted web site, as demonstrated by an array-redimensioning attempt that triggers improper handling of a size value in the SafeArrayDimen function, aka ""Windows OLE Automation Array Remote Code Execution Vulnerability."""  
  
[CVE-2014-6352] Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document.  
  
[CVE-2014-6355] "The Graphics Component in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly process JPEG images, which makes it easier for remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka ""Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2015-0001] "The Windows Error Reporting (WER) component in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to bypass the Protected Process Light protection mechanism and read the contents of arbitrary process-memory locations by leveraging administrative privileges, aka ""Windows Error Reporting Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0002] "The AhcVerifyAdminContext function in ahcache.sys in the Application Compatibility component in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not verify that an impersonation token is associated with an administrative account, which allows local users to gain privileges by running AppCompatCache.exe with a crafted DLL file, aka MSRC ID 20544 or ""Microsoft Application Compatibility Infrastructure Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0003] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0004] "The User Profile Service (aka ProfSvc) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges by conducting a junction attack to load another user's UsrClass.dat registry hive, aka MSRC ID 20674 or ""Microsoft User Profile Service Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0005] "The NETLOGON service in Microsoft Windows Server 2003 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2, when a Domain Controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, aka ""NETLOGON Spoofing Vulnerability."""  
  
[CVE-2015-0006] "The Network Location Awareness (NLA) service in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not perform mutual authentication to determine a domain connection, which allows remote attackers to trigger an unintended permissive configuration by spoofing DNS and LDAP responses on a local network, aka ""NLA Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0008] "The UNC implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not include authentication from the server to the client, which allows remote attackers to execute arbitrary code by making crafted data available on a UNC share, as demonstrated by Group Policy data from a spoofed domain controller, aka ""Group Policy Remote Code Execution Vulnerability."""  
  
[CVE-2015-0009] "The Group Policy Security Configuration policy implementation in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows man-in-the-middle attackers to disable a signing requirement and trigger a revert-to-default action by spoofing domain-controller responses, aka ""Group Policy Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0010] "The CryptProtectMemory function in cng.sys (aka the Cryptography Next Generation driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1, when the CRYPTPROTECTMEMORY\_SAME\_LOGON option is used, does not check an impersonation token's level, which allows local users to bypass intended decryption restrictions by leveraging a service that (1) has a named-pipe planting vulnerability or (2) uses world-readable shared memory for encrypted data, aka ""CNG Security Feature Bypass Vulnerability"" or MSRC ID 20707."  
  
[CVE-2015-0011] "mrxdav.sys (aka the WebDAV driver) in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to bypass an impersonation protection mechanism, and obtain privileges for redirection of WebDAV requests, via a crafted application, aka ""WebDAV Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0014] "Buffer overflow in the Telnet service in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted packets, aka ""Windows Telnet Service Buffer Overflow Vulnerability."""  
  
[CVE-2015-0015] "Microsoft Windows Server 2003 SP2, Server 2008 SP2 and R2 SP1, and Server 2012 Gold and R2 allow remote attackers to cause a denial of service (system hang and RADIUS outage) via crafted username strings to (1) Internet Authentication Service (IAS) or (2) Network Policy Server (NPS), aka ""Network Policy Server RADIUS Implementation Denial of Service Vulnerability."""  
  
[CVE-2015-0016] "Directory traversal vulnerability in the TS WebProxy (aka TSWbPrxy) component in Microsoft Windows Vista SP2, Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via a crafted pathname in an executable file, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""Directory Traversal Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0057] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0058] "Double free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows local users to gain privileges via a crafted application, aka ""Windows Cursor Object Double Free Vulnerability."""  
  
[CVE-2015-0059] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted TrueType font, aka ""TrueType Font Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2015-0060] "The font mapper in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly scale fonts, which allows local users to cause a denial of service (system hang) via a crafted application, aka ""Windows Font Driver Denial of Service Vulnerability."""  
  
[CVE-2015-0061] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize memory for TIFF images, which allows remote attackers to obtain sensitive information from process memory via a crafted image file, aka ""TIFF Processing Information Disclosure Vulnerability."""  
  
[CVE-2015-0062] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to gain privileges via a crafted application that leverages incorrect impersonation handling in a process that uses the SeAssignPrimaryTokenPrivilege privilege, aka ""Windows Create Process Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0073] "The Windows Registry Virtualization feature in the kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict changes to virtual stores, which allows local users to gain privileges via a crafted application, aka ""Registry Virtualization Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0074] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly allocate memory, which allows remote attackers to cause a denial of service via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Denial of Service Vulnerability."""  
  
[CVE-2015-0075] "The kernel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Impersonation Level Check Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0076] "The photo-decoder implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly initialize memory for rendering of JXR images, which allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""JPEG XR Parser Information Disclosure Vulnerability."""  
  
[CVE-2015-0077] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize function buffers, which allows local users to obtain sensitive information from kernel memory, and possibly bypass the ASLR protection mechanism, via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0078] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate the token of a calling thread, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-0079] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to cause a denial of service (memory consumption and RDP outage) by establishing many RDP sessions that do not properly free allocated memory, aka ""Remote Desktop Protocol (RDP) Denial of Service Vulnerability."""  
  
[CVE-2015-0080] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly initialize memory for rendering of malformed PNG images, which allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Malformed PNG Parsing Information Disclosure Vulnerability."""  
  
[CVE-2015-0081] "Windows Text Services (WTS) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""WTS Remote Code Execution Vulnerability."""  
  
[CVE-2015-0084] "The Task Scheduler in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to bypass intended restrictions on launching executable files via a crafted task, aka ""Task Scheduler Security Feature Bypass Vulnerability."""  
  
[CVE-2015-0085] "Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Excel Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Server 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePoint Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, and SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka ""Microsoft Office Component Use After Free Vulnerability."""  
  
[CVE-2015-0087] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive information from kernel memory, and possibly bypass the KASLR protection mechanism, via a crafted font, aka ""Adobe Font Driver Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-0089."  
  
[CVE-2015-0088] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0089] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive information from kernel memory, and possibly bypass the KASLR protection mechanism, via a crafted font, aka ""Adobe Font Driver Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-0087."  
  
[CVE-2015-0090] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0091, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0091] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0092, and CVE-2015-0093."  
  
[CVE-2015-0092] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0093."  
  
[CVE-2015-0093] "Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka ""Adobe Font Driver Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, and CVE-2015-0092."  
  
[CVE-2015-0094] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly restrict the availability of address information during a function call, which makes it easier for local users to bypass the ASLR protection mechanism via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0095] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to cause a denial of service (NULL pointer dereference and blue screen), or obtain sensitive information from kernel memory and possibly bypass the ASLR protection mechanism, via a crafted application, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability."""  
  
[CVE-2015-0096] "Untrusted search path vulnerability in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, leading to DLL loading during Windows Explorer access to the icon of a crafted shortcut, aka ""DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-0098] "Task Scheduler in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges by triggering application execution by an invalid task, aka ""Task Scheduler Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1635] "HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka ""HTTP.sys Remote Code Execution Vulnerability."""  
  
[CVE-2015-1637] "Schannel (aka Secure Channel) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict TLS state transitions, which makes it easier for remote attackers to conduct cipher-downgrade attacks to EXPORT\_RSA ciphers via crafted TLS traffic, related to the ""FREAK"" issue, a different vulnerability than CVE-2015-0204 and CVE-2015-1067."  
  
[CVE-2015-1638] "Microsoft Active Directory Federation Services (AD FS) 3.0 on Windows Server 2012 R2 does not properly handle logoff actions, which allows remote attackers to bypass intended access restrictions by leveraging an unattended workstation, aka ""Active Directory Federation Services Information Disclosure Vulnerability."""  
  
[CVE-2015-1643] "Microsoft Windows Server 2003 R2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""NtCreateTransactionManager Type Confusion Vulnerability."""  
  
[CVE-2015-1644] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows MS-DOS Device Name Vulnerability."""  
  
[CVE-2015-1645] "Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to execute arbitrary code via a crafted Enhanced Metafile (EMF) image, aka ""EMF Processing Remote Code Execution Vulnerability."""  
  
[CVE-2015-1647] "Virtual Machine Manager (VMM) in Hyper-V in Microsoft Windows 8.1 and Windows Server 2012 R2 allows guest OS users to cause a denial of service (VMM functionality loss) via a crafted application, aka ""Windows Hyper-V DoS Vulnerability."""  
  
[CVE-2015-1670] "The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2, allows remote attackers to obtain sensitive information from process memory via a crafted OpenType font on a web site, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-1671] "The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2  
[CVE-2015-1673] "The Windows Forms (aka WinForms) libraries in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2 allow user-assisted remote attackers to execute arbitrary code via a crafted partial-trust application, aka ""Windows Forms Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1674] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate an unspecified address, which allows local users to bypass the KASLR protection mechanism, and consequently discover the cng.sys base address, via a crafted application, aka ""Windows Kernel Security Feature Bypass Vulnerability."""  
  
[CVE-2015-1675] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1676] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1677, CVE-2015-1678, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1677] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1678, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1678] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1679, and CVE-2015-1680."  
  
[CVE-2015-1679] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, and CVE-2015-1680."  
  
[CVE-2015-1680] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to bypass the ASLR protection mechanism via a crafted function call, aka ""Microsoft Windows Kernel Memory Disclosure Vulnerability,"" a different vulnerability than CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, and CVE-2015-1679."  
  
[CVE-2015-1681] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to cause a denial of service via a crafted .msc file, aka ""Microsoft Management Console File Format Denial of Service Vulnerability."""  
  
[CVE-2015-1695] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1696] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1697] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1698, and CVE-2015-1699."  
  
[CVE-2015-1698] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1699."  
  
[CVE-2015-1699] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1698."  
  
[CVE-2015-1701] "Win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows local users to gain privileges via a crafted application, as exploited in the wild in April 2015, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1702] "The Service Control Manager (SCM) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Service Control Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1716] "Schannel in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly restrict Diffie-Hellman Ephemeral (DHE) key lengths, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, aka ""Schannel Information Disclosure Vulnerability."""  
  
[CVE-2015-1719] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to obtain sensitive information from kernel memory via a crafted application, aka ""Microsoft Windows Kernel Information Disclosure Vulnerability."""  
  
[CVE-2015-1720] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Use After Free Vulnerability."""  
  
[CVE-2015-1721] "The kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka ""Win32k Null Pointer Dereference Vulnerability."""  
  
[CVE-2015-1722] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Bitmap Handling Use After Free Vulnerability."""  
  
[CVE-2015-1723] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Station Use After Free Vulnerability."""  
  
[CVE-2015-1724] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Object Use After Free Vulnerability."""  
  
[CVE-2015-1725] "Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Buffer Overflow Vulnerability."""  
  
[CVE-2015-1726] "Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Microsoft Windows Kernel Brush Object Use After Free Vulnerability."""  
  
[CVE-2015-1727] "Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Pool Buffer Overflow Vulnerability."""  
  
[CVE-2015-1728] "Microsoft Windows Media Player 10 through 12 allows remote attackers to execute arbitrary code via a crafted DataObject on a web site, aka ""Windows Media Player RCE via DataObject Vulnerability."""  
  
[CVE-2015-1756] "Use-after-free vulnerability in Microsoft Common Controls in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted web site that is accessed with the F12 Developer Tools feature of Internet Explorer, aka ""Microsoft Common Control Use After Free Vulnerability."""  
  
[CVE-2015-1757] "Cross-site scripting (XSS) vulnerability in adfs/ls in Active Directory Federation Services (AD FS) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 allows remote attackers to inject arbitrary web script or HTML via the wct parameter, aka ""ADFS XSS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1758] "Untrusted search path vulnerability in the LoadLibrary function in the kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a Trojan horse DLL in an unspecified directory, aka ""Windows LoadLibrary EoP Vulnerability."""  
  
[CVE-2015-1768] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability."""  
  
[CVE-2015-1769] "Mount Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 mishandles symlinks, which allows physically proximate attackers to execute arbitrary code by connecting a crafted USB device, aka ""Mount Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2360] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2361] "Hyper-V in Microsoft Windows 8.1 and Windows Server 2012 R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (buffer overflow) by leveraging guest OS privileges, aka ""Hyper-V Buffer Overflow Vulnerability."""  
  
[CVE-2015-2362] "Hyper-V in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS by leveraging guest OS privileges, aka ""Hyper-V System Data Structure Vulnerability."""  
  
[CVE-2015-2363] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2364] "The graphics component in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application that leverages an incorrect bitmap conversion, aka ""Graphics Component EOP Vulnerability."""  
  
[CVE-2015-2365] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2366] "win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2367] "win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from uninitialized kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2015-2368] "Untrusted search path vulnerability in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka ""Windows DLL Remote Code Execution Vulnerability."""  
  
[CVE-2015-2369] "Untrusted search path vulnerability in Windows Media Device Manager in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rtf file, aka ""DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-2371] "The Windows Installer service in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a custom action script associated with a .msi package, aka ""Windows Installer EoP Vulnerability."""  
  
[CVE-2015-2373] "The Remote Desktop Protocol (RDP) server service in Microsoft Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a series of crafted packets, aka ""Remote Desktop Protocol (RDP) Remote Code Execution Vulnerability."""  
  
[CVE-2015-2374] "The Netlogon service in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 Gold and R2 does not properly implement domain-controller communication, which allows remote attackers to discover credentials by leveraging certain PDC access and spoofing the BDC role in a PDC communication channel, aka ""Elevation of Privilege Vulnerability in Netlogon."""  
  
[CVE-2015-2381] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-2382."  
  
[CVE-2015-2382] "win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information from kernel memory via a crafted application, aka ""Win32k Information Disclosure Vulnerability,"" a different vulnerability than CVE-2015-2381."  
  
[CVE-2015-2387] "ATMFD.DLL in the Adobe Type Manager Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka ""ATMFD.DLL Memory Corruption Vulnerability."""  
  
[CVE-2015-2416] "OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via crafted input, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""OLE Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2417."  
  
[CVE-2015-2417] "OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to gain privileges via crafted input, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""OLE Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2416."  
  
[CVE-2015-2423] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Excel 2007 SP3, PowerPoint 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Visio 2013 RT SP1, Word 2013 RT SP1, and Internet Explorer 7 through 11 allow remote attackers to gain privileges and obtain sensitive information via a crafted command-line parameter to an Office application or Notepad, as demonstrated by a transition from Low Integrity to Medium Integrity, aka ""Unsafe Command Line Parameter Passing Vulnerability."""  
  
[CVE-2015-2426] "Buffer underflow in atmfd.dll in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Driver Vulnerability."""  
  
[CVE-2015-2428] "Object Manager in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels during interaction with object symbolic links that originated in a sandboxed process, which allows local users to gain privileges via a crafted application, aka ""Windows Object Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2429] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow attackers to bypass an application sandbox protection mechanism and perform unspecified registry actions via a crafted application, aka ""Windows Registry Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2430] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow attackers to bypass an application sandbox protection mechanism and perform unspecified filesystem actions via a crafted application, aka ""Windows Filesystem Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2432] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2433] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""Kernel ASLR Bypass Vulnerability."""  
  
[CVE-2015-2435] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Silverlight before 5.1.40728 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability."""  
  
[CVE-2015-2453] "The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information via a crafted application that continues to execute during a subsequent user's login session, aka ""Windows CSRSS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2454] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows KMD Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2455] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2456."  
  
[CVE-2015-2456] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2455."  
  
[CVE-2015-2458] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2459 and CVE-2015-2461."  
  
[CVE-2015-2459] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2458 and CVE-2015-2461."  
  
[CVE-2015-2460] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2461] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2458 and CVE-2015-2459."  
  
[CVE-2015-2462] "ATMFD.DLL in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2463] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2464."  
  
[CVE-2015-2464] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP2, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, Silverlight before 5.1.40728, and .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 allow remote attackers to execute arbitrary code via a crafted TrueType font, aka ""TrueType Font Parsing Vulnerability,"" a different vulnerability than CVE-2015-2463."  
  
[CVE-2015-2465] "The Windows shell in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Shell Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2472] "Remote Desktop Session Host (RDSH) in Remote Desktop Protocol (RDP) through 8.1 in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly verify certificates, which allows man-in-the-middle attackers to spoof clients via a crafted certificate with valid Issuer and Serial Number fields, aka ""Remote Desktop Session Host Spoofing Vulnerability."""  
  
[CVE-2015-2473] "Untrusted search path vulnerability in the client in Remote Desktop Protocol (RDP) through 8.1 in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .rdp file, aka ""Remote Desktop Protocol DLL Planting Remote Code Execution Vulnerability."""  
  
[CVE-2015-2474] "Microsoft Windows Vista SP2 and Server 2008 SP2 allow remote authenticated users to execute arbitrary code via a crafted string in a Server Message Block (SMB) server error-logging action, aka ""Server Message Block Memory Corruption Vulnerability."""  
  
[CVE-2015-2475] "Cross-site scripting (XSS) vulnerability in uddi/search/frames.aspx in the UDDI Services component in Microsoft Windows Server 2008 SP2 and BizTalk Server 2010, 2013 Gold, and 2013 R2 allows remote attackers to inject arbitrary web script or HTML via the search parameter, aka ""UDDI Services Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2476] "The WebDAV client in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 supports SSL 2.0, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and conducting a decryption attack, aka ""WebDAV Client Information Disclosure Vulnerability."""  
  
[CVE-2015-2478] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application that triggers a Winsock call referencing an invalid address, aka ""Winsock Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2506] "atmfd.dll in the Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to cause a denial of service (system crash) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2015-2507] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2512."  
  
[CVE-2015-2508] "The Adobe Type Manager Library in Microsoft Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2509] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted Media Center link (mcl) file, aka ""Windows Media Center RCE Vulnerability."""  
  
[CVE-2015-2510] "Buffer overflow in the Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""Graphics Component Buffer Overflow Vulnerability."""  
  
[CVE-2015-2511] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2517, CVE-2015-2518, and CVE-2015-2546."  
  
[CVE-2015-2512] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Font Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2507."  
  
[CVE-2015-2513] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2514 and CVE-2015-2530."  
  
[CVE-2015-2514] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2513 and CVE-2015-2530."  
  
[CVE-2015-2515] "Use-after-free vulnerability in Windows Shell in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted toolbar object, aka ""Toolbar Use After Free Vulnerability."""  
  
[CVE-2015-2516] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to cause a denial of service (data loss) via a crafted .jnt file, aka ""Windows Journal DoS Vulnerability."""  
  
[CVE-2015-2517] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2518, and CVE-2015-2546."  
  
[CVE-2015-2518] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2546."  
  
[CVE-2015-2519] "Integer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal Integer Overflow RCE Vulnerability."""  
  
[CVE-2015-2524] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Task Management Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2528."  
  
[CVE-2015-2525] "Task Scheduler in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to bypass intended filesystem restrictions and delete arbitrary files via unspecified vectors, aka ""Windows Task File Deletion Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2527] "The process-initialization implementation in win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2528] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka ""Windows Task Management Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2524."  
  
[CVE-2015-2529] "The kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""Kernel ASLR Bypass Vulnerability."""  
  
[CVE-2015-2530] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka ""Windows Journal RCE Vulnerability,"" a different vulnerability than CVE-2015-2513 and CVE-2015-2514."  
  
[CVE-2015-2534] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows 10 improperly processes ACL settings, which allows local users to bypass intended network-traffic restrictions via a crafted application, aka ""Hyper-V Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2535] "Active Directory in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (service outage) by creating multiple machine accounts, aka ""Active Directory Denial of Service Vulnerability."""  
  
[CVE-2015-2546] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Win32k Memory Corruption Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2518."  
  
[CVE-2015-2548] "Use-after-free vulnerability in the Tablet Input Band in Windows Shell in Microsoft Windows Vista SP2 and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Microsoft Tablet Input Band Use After Free Vulnerability."""  
  
[CVE-2015-2549] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Corruption Vulnerability."""  
  
[CVE-2015-2550] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2552] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows physically proximate attackers to bypass the Trusted Boot protection mechanism, and consequently interfere with the integrity of code, BitLocker, Device Encryption, and Device Health Attestation, via a crafted Boot Configuration Data (BCD) setting, aka ""Trusted Boot Security Feature Bypass Vulnerability."""  
  
[CVE-2015-2553] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 mishandles junctions during mountpoint creation, which makes it easier for local users to gain privileges by leveraging certain sandbox access, aka ""Windows Mount Point Elevation of Privilege Vulnerability."""  
  
[CVE-2015-2554] "The kernel in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka ""Windows Object Reference Elevation of Privilege Vulnerability."""  
  
[CVE-2015-4949] IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server 7.1 before 7.1.2, Tivoli Storage Manager for Mail: Data Protection for Microsoft Exchange Server 7.1 before 7.1.2, and Tivoli Storage FlashCopy Manager 4.1 before 4.1.2 place cleartext passwords in exception messages, which allows physically proximate attackers to obtain sensitive information by reading GUI pop-up windows, a different vulnerability than CVE-2015-6557.  
  
[CVE-2015-6095] "Kerberos in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles password changes, which allows physically proximate attackers to bypass authentication, and conduct decryption attacks against certain BitLocker configurations, by connecting to an unintended Key Distribution Center (KDC), aka ""Windows Kerberos Security Feature Bypass."""  
  
[CVE-2015-6097] "Heap-based buffer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted Journal (.jnt) file, aka ""Windows Journal Heap Overflow Vulnerability."""  
  
[CVE-2015-6098] "Buffer overflow in the Network Driver Interface Standard (NDIS) implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""Windows NDIS Elevation of Privilege Vulnerability."""  
  
[CVE-2015-6100] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6101."  
  
[CVE-2015-6101] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6100."  
  
[CVE-2015-6102] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to bypass the KASLR protection mechanism, and consequently discover a driver base address, via a crafted application, aka ""Windows Kernel Memory Information Disclosure Vulnerability."""  
  
[CVE-2015-6103] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-6104."  
  
[CVE-2015-6104] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2015-6103."  
  
[CVE-2015-6106] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Graphics Memory Corruption Vulnerability."""  
  
[CVE-2015-6107] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10 Gold and 1511, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Graphics Memory Corruption Vulnerability."""  
  
[CVE-2015-6108] "The Windows font library in Microsoft Windows Vista SP2  
[CVE-2015-6109] "The kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the KASLR protection mechanism, and consequently discover a driver base address, via a crafted application, aka ""Windows Kernel Memory Information Disclosure Vulnerability."""  
  
[CVE-2015-6111] "IPSec in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles encryption negotiation, which allows remote authenticated users to cause a denial of service (system hang) via crafted IP traffic, aka ""Windows IPSec Denial of Service Vulnerability."""  
  
[CVE-2015-6112] "SChannel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 lacks the required extended master-secret binding support to ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers to obtain sensitive information or modify TLS session data via a ""triple handshake attack,"" aka ""Schannel TLS Triple Handshake Vulnerability."""  
  
[CVE-2015-6113] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to bypass intended filesystem permissions by leveraging Low Integrity access, aka ""Windows Kernel Security Feature Bypass Vulnerability."""  
  
[CVE-2015-6125] "Use-after-free vulnerability in the DNS server in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka ""Windows DNS Use After Free Vulnerability."""  
  
[CVE-2015-6126] "Race condition in the Pragmatic General Multicast (PGM) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application, aka ""Windows PGM UAF Elevation of Privilege Vulnerability."""  
  
[CVE-2015-6127] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows remote attackers to read arbitrary files via a crafted .mcl file, aka ""Windows Media Center Information Disclosure Vulnerability."""  
  
[CVE-2015-6128] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6130] "Integer underflow in Uniscribe in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows remote attackers to execute arbitrary code via a crafted font, aka ""Windows Integer Underflow Vulnerability."""  
  
[CVE-2015-6131] "Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted .mcl file, aka ""Media Center Library Parsing RCE Vulnerability."""  
  
[CVE-2015-6132] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6133] "Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Library Loading Remote Code Execution Vulnerability."""  
  
[CVE-2015-6171] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6173 and CVE-2015-6174."  
  
[CVE-2015-6173] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6171 and CVE-2015-6174."  
  
[CVE-2015-6174] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2015-6171 and CVE-2015-6173."  
  
[CVE-2015-6175] "The kernel in Microsoft Windows 10 Gold allows local users to gain privileges via a crafted application, aka ""Windows Kernel Memory Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0006] "The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka ""Windows Mount Point Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0007."  
  
[CVE-2016-0007] "The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka ""Windows Mount Point Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0006."  
  
[CVE-2016-0008] "The graphics device interface in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka ""Windows GDI32.dll ASLR Bypass Vulnerability."""  
  
[CVE-2016-0009] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via unspecified vectors, aka ""Win32k Remote Code Execution Vulnerability."""  
  
[CVE-2016-0014] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0015] "DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""DirectShow Heap Corruption Remote Code Execution Vulnerability."""  
  
[CVE-2016-0016] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0018] "Microsoft Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 R2, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0019] "The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka ""Windows Remote Desktop Protocol Security Bypass Vulnerability."""  
  
[CVE-2016-0020] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""MAPI DLL Loading Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0026] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-0036] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote authenticated users to execute arbitrary code via crafted data, aka ""Remote Desktop Protocol (RDP) Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0037] "The forms-based authentication implementation in Active Directory Federation Services (ADFS) 3.0 in Microsoft Windows Server 2012 R2 allows remote attackers to cause a denial of service (daemon outage) via crafted data, aka ""Microsoft Active Directory Federation Services Denial of Service Vulnerability."""  
  
[CVE-2016-0038] "Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal file, aka ""Windows Journal Memory Corruption Vulnerability."""  
  
[CVE-2016-0040] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0041] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 10 and 11 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0042] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka ""Windows DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0044] "Sync Framework in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1 allows remote attackers to cause a denial of service (SyncShareSvc service outage) via crafted ""change batch"" data, aka ""Windows DLL Loading Denial of Service Vulnerability."""  
  
[CVE-2016-0046] "Windows Reader in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted Reader file, aka ""Microsoft Windows Reader Vulnerability."""  
  
[CVE-2016-0047] "WinForms in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 allows remote attackers to obtain sensitive information from process memory via crafted icon data, aka ""Windows Forms Information Disclosure Vulnerability."""  
  
[CVE-2016-0048] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0049] "Kerberos in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 does not properly validate password changes, which allows remote attackers to bypass authentication by deploying a crafted Key Distribution Center (KDC) and then performing a sign-in action, aka ""Windows Kerberos Security Feature Bypass."""  
  
[CVE-2016-0050] "Network Policy Server (NPS) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 misparses username queries, which allows remote attackers to cause a denial of service (RADIUS authentication outage) via crafted requests, aka ""Network Policy Server RADIUS Implementation Denial of Service Vulnerability."""  
  
[CVE-2016-0051] "The WebDAV client in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""WebDAV Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0058] "Buffer overflow in the PDF Library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted PDF document that triggers API calls, aka ""Microsoft PDF Library Buffer Overflow Vulnerability."""  
  
[CVE-2016-0070] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0073] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0075."  
  
[CVE-2016-0075] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0073."  
  
[CVE-2016-0079] "The kernel in Microsoft Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application that makes an API call to access sensitive information in the registry, aka ""Windows Kernel Local Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0087] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 do not properly validate handles, which allows local users to gain privileges via a crafted application, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0088] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows guest OS users to execute arbitrary code on the host OS via a crafted application, aka ""Hyper-V Remote Code Execution Vulnerability."""  
  
[CVE-2016-0089] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows guest OS users to obtain sensitive information from host OS memory via a crafted application, aka ""Hyper-V Information Disclosure Vulnerability."""  
  
[CVE-2016-0090] "Hyper-V in Microsoft Windows 8.1, Windows Server 2012 R2, and Windows 10 allows guest OS users to obtain sensitive information from host OS memory via a crafted application, aka ""Hyper-V Information Disclosure Vulnerability."""  
  
[CVE-2016-0091] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2016-0092."  
  
[CVE-2016-0092] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Memory Remote Code Execution Vulnerability,"" a different vulnerability than CVE-2016-0091."  
  
[CVE-2016-0093] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0094, CVE-2016-0095, and CVE-2016-0096."  
  
[CVE-2016-0094] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0095, and CVE-2016-0096."  
  
[CVE-2016-0095] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0096."  
  
[CVE-2016-0096] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0095."  
  
[CVE-2016-0098] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 allow remote attackers to execute arbitrary code via crafted media content, aka ""Windows Media Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2016-0099] "The Secondary Logon Service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 does not properly process request handles, which allows local users to gain privileges via a crafted application, aka ""Secondary Logon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0100] "Microsoft Windows Vista SP2 and Server 2008 SP2 mishandle library loading, which allows local users to gain privileges via a crafted application, aka ""Library Loading Input Validation Remote Code Execution Vulnerability."""  
  
[CVE-2016-0101] "Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via crafted media content, aka ""Windows Media Parsing Remote Code Execution Vulnerability."""  
  
[CVE-2016-0117] "The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-0118] "The PDF library in Microsoft Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-0120] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2016-0121] "The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka ""OpenType Font Parsing Vulnerability."""  
  
[CVE-2016-0133] "The USB Mass Storage Class driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows physically proximate attackers to execute arbitrary code by inserting a crafted USB device, aka ""USB Mass Storage Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0135] "The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Secondary Logon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0142] "Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted web page, aka ""Microsoft Video Control Remote Code Execution Vulnerability."""  
  
[CVE-2016-0143] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0165 and CVE-2016-0167."  
  
[CVE-2016-0145] "The font library in Microsoft Windows Vista SP2  
[CVE-2016-0150] "HTTP.sys in Microsoft Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via crafted HTTP 2.0 requests, aka ""HTTP.sys Denial of Service Vulnerability."""  
  
[CVE-2016-0151] "The Client-Server Run-time Subsystem (CSRSS) in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mismanages process tokens, which allows local users to gain privileges via a crafted application, aka ""Windows CSRSS Security Feature Bypass Vulnerability."""  
  
[CVE-2016-0152] "Internet Information Services (IIS) in Microsoft Windows Vista SP2 and Server 2008 SP2 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows DLL Loading Remote Code Execution Vulnerability."""  
  
[CVE-2016-0153] "OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows remote attackers to execute arbitrary code via a crafted file, aka ""Windows OLE Remote Code Execution Vulnerability."""  
  
[CVE-2016-0165] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0143 and CVE-2016-0167."  
  
[CVE-2016-0167] "The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0143 and CVE-2016-0165."  
  
[CVE-2016-0168] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to obtain sensitive information via a crafted document, aka ""Windows Graphics Component Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-0169."  
  
[CVE-2016-0169] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to obtain sensitive information via a crafted document, aka ""Windows Graphics Component Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-0168."  
  
[CVE-2016-0170] "GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Windows Graphics Component RCE Vulnerability."""  
  
[CVE-2016-0171] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0173, CVE-2016-0174, and CVE-2016-0196."  
  
[CVE-2016-0173] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0174, and CVE-2016-0196."  
  
[CVE-2016-0174] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0196."  
  
[CVE-2016-0175] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to obtain sensitive information about kernel-object addresses, and consequently bypass the KASLR protection mechanism, via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-0176] "dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0179] "Windows Shell in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Shell Remote Code Execution Vulnerability."""  
  
[CVE-2016-0180] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles symbolic links, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-0181] "Microsoft Windows 10 Gold and 1511 allows local users to bypass the Virtual Secure Mode Hypervisor Code Integrity (HVCI) protection mechanism and perform RWX markings of kernel-mode pages via a crafted application, aka ""Hypervisor Code Integrity Security Feature Bypass."""  
  
[CVE-2016-0182] "Windows Journal in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal (aka .jnt) file, aka ""Windows Journal Memory Corruption Vulnerability."""  
  
[CVE-2016-0183] "The Windows font library in Microsoft Office 2010 SP2, Word 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Microsoft Office Graphics RCE Vulnerability."""  
  
[CVE-2016-0184] "Use-after-free vulnerability in GDI in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Direct3D Use After Free Vulnerability."""  
  
[CVE-2016-0185] "Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted Media Center link (aka .mcl) file, aka ""Windows Media Center Remote Code Execution Vulnerability."""  
  
[CVE-2016-0190] "Volume Manager Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 does not properly check whether RemoteFX RDP USB disk accesses originate from the user who mounted a disk, which allows local users to read arbitrary files on these disks via RemoteFX requests, aka ""Remote Desktop Protocol Drive Redirection Information Disclosure Vulnerability."""  
  
[CVE-2016-0195] "The Imaging Component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted document, aka ""Windows Imaging Component Memory Corruption Vulnerability."""  
  
[CVE-2016-0196] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0174."  
  
[CVE-2016-0197] "dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3201] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka ""Windows PDF Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3215."  
  
[CVE-2016-3203] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to execute arbitrary code via a crafted PDF document, aka ""Windows PDF Remote Code Execution Vulnerability."""  
  
[CVE-2016-3209] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3213] "The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, and Internet Explorer 9 through 11 has an improper fallback mechanism, which allows remote attackers to gain privileges via NetBIOS name responses, aka ""WPAD Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3215] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka ""Windows PDF Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3201."  
  
[CVE-2016-3216] "GDI32.dll in the Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka ""Windows Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2016-3218] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3221."  
  
[CVE-2016-3219] "The kernel-mode driver in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3220] "atmfd.dll in the Adobe Type Manager Font Driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka ""ATMFD.dll Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3221] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3218."  
  
[CVE-2016-3223] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandle LDAP authentication, which allows man-in-the-middle attackers to gain privileges by modifying group-policy update data within a domain-controller data stream, aka ""Group Policy Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3225] "The SMB server component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application that forwards an authentication request to an unintended service, aka ""Windows SMB Server Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3226] "Active Directory in Microsoft Windows Server 2008 R2 SP1 and Server 2012 Gold and R2 allows remote authenticated users to cause a denial of service (service hang) by creating many machine accounts, aka ""Active Directory Denial of Service Vulnerability."""  
  
[CVE-2016-3227] "Use-after-free vulnerability in the DNS Server component in Microsoft Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka ""Windows DNS Server Use After Free Vulnerability."""  
  
[CVE-2016-3228] "Microsoft Windows Server 2008 SP2 and R2 SP1 and Windows Server 2012 Gold and R2 allow remote authenticated users to execute arbitrary code via a crafted NetLogon request, aka ""Windows Netlogon Memory Corruption Remote Code Execution Vulnerability."""  
  
[CVE-2016-3230] "The Search component in Microsoft Windows 7, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to cause a denial of service (performance degradation) via a crafted application, aka ""Windows Search Component Denial of Service Vulnerability."""  
  
[CVE-2016-3232] "The Virtual PCI (VPCI) virtual service provider in Microsoft Windows Server 2012 Gold and R2 allows local users to obtain sensitive information from uninitialized memory locations via a crafted application, aka ""Windows Virtual PCI Information Disclosure Vulnerability."""  
  
[CVE-2016-3236] "The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka ""Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3237] "Kerberos in Microsoft Windows Vista SP2  
[CVE-2016-3238] "The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows man-in-the-middle attackers to execute arbitrary code by providing a crafted print driver during printer installation, aka ""Windows Print Spooler Remote Code Execution Vulnerability."""  
  
[CVE-2016-3239] "The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via vectors involving filesystem write operations, aka ""Windows Print Spooler Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3249] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3252, CVE-2016-3254, and CVE-2016-3286."  
  
[CVE-2016-3250] "The kernel-mode drivers in Microsoft Windows Server 2012 and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3251] "The GDI component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to obtain sensitive kernel-address information via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-3252] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3254, and CVE-2016-3286."  
  
[CVE-2016-3254] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3286."  
  
[CVE-2016-3256] "Microsoft Windows 10 Gold and 1511 allows local users to bypass the Secure Kernel Mode protection mechanism and obtain sensitive information via a crafted application, aka ""Windows Secure Kernel Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-3258] "Race condition in the kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Low Integrity protection mechanism and write to files by leveraging unspecified object-manager features, aka ""Windows File System Security Feature Bypass."""  
  
[CVE-2016-3262] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3263] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3266] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3376, CVE-2016-7185, and CVE-2016-7211."  
  
[CVE-2016-3270] "The Graphics component in the kernel in Microsoft Windows Vista SP2  
[CVE-2016-3272] "The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles page-fault system calls, which allows local users to obtain sensitive information from an arbitrary process via a crafted application, aka ""Windows Kernel Information Disclosure Vulnerability."""  
  
[CVE-2016-3286] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3254."  
  
[CVE-2016-3287] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Secure Boot protection mechanism by leveraging administrative access to install a crafted policy, aka ""Secure Boot Security Feature Bypass."""  
  
[CVE-2016-3298] "Microsoft Internet Explorer 9 through 11 and the Internet Messaging API in Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allow remote attackers to determine the existence of arbitrary files via a crafted web site, aka ""Internet Explorer Information Disclosure Vulnerability."""  
  
[CVE-2016-3299] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to hijack network traffic or bypass intended Enhanced Protected Mode (EPM) or application container protection mechanisms, and consequently render untrusted content in a browser, by leveraging how NetBIOS validates responses, aka ""NetBIOS Spoofing Vulnerability."""  
  
[CVE-2016-3300] "The Netlogon service in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 improperly establishes secure communications channels, which allows local users to gain privileges by leveraging access to a domain-joined machine, aka ""Netlogon Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3301] "The Windows font library in Microsoft Windows Vista SP2  
[CVE-2016-3302] "Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607, when the lock screen is enabled, do not properly restrict the loading of web content, which allows physically proximate attackers to execute arbitrary code via a (1) crafted Wi-Fi access point or (2) crafted mobile-broadband device, aka ""Windows Lock Screen Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3303] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Component RCE Vulnerability,"" a different vulnerability than CVE-2016-3304."  
  
[CVE-2016-3304] "The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka ""Windows Graphics Component RCE Vulnerability,"" a different vulnerability than CVE-2016-3303."  
  
[CVE-2016-3305] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka ""Windows Session Object Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3306."  
  
[CVE-2016-3306] "The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka ""Windows Session Object Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-3305."  
  
[CVE-2016-3308] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3309] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3310] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3311] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2016-3312] "ActiveSyncProvider in Microsoft Windows 10 Gold and 1511 allows attackers to discover credentials by leveraging failure of Universal Outlook to obtain a secure connection, aka ""Universal Outlook Information Disclosure Vulnerability."""  
  
[CVE-2016-3319] "The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allows remote attackers to execute arbitrary code via a crafted PDF file, aka ""Microsoft PDF Remote Code Execution Vulnerability."""  
  
[CVE-2016-3320] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow attackers to bypass the Secure Boot protection mechanism by leveraging (1) administrative or (2) physical access to install a crafted boot manager, aka ""Secure Boot Security Feature Bypass."""  
  
[CVE-2016-3332] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3333] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3334] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3335] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3338] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3340] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3341] "The kernel-mode drivers in Transaction Manager in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Windows Transaction Manager Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3342] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3343, and CVE-2016-7184."  
  
[CVE-2016-3343] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-7184."  
  
[CVE-2016-3344] "The Secure Kernel Mode feature in Microsoft Windows 10 Gold and 1511 allows local users to obtain sensitive information via a crafted application, aka ""Windows Secure Kernel Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-3345] "The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via crafted packets, aka ""Windows SMB Authenticated Remote Code Execution Vulnerability."""  
  
[CVE-2016-3346] "Microsoft Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain Administrator access via a crafted DLL, aka ""Windows Permissions Enforcement Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3348] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3349] "The kernel-mode drivers in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3352] "Microsoft Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 do not properly check NTLM SSO requests for MSA logins, which makes it easier for remote attackers to determine passwords via a brute-force attack on NTLM password hashes, aka ""Microsoft Information Disclosure Vulnerability."""  
  
[CVE-2016-3354] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to bypass the ASLR protection mechanism via a crafted application, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2016-3355] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka ""GDI Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3356] "The Graphics Device Interface (GDI) in Microsoft Windows 10 1607 allows remote attackers to execute arbitrary code via a crafted document, aka ""GDI Remote Code Execution Vulnerability."""  
  
[CVE-2016-3368] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote authenticated users to execute arbitrary code by leveraging a domain account to make a crafted request, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-3369] "Microsoft Windows 10 Gold and 1511 allows attackers to cause a denial of service via unspecified vectors, aka ""Windows Denial of Service Vulnerability."""  
  
[CVE-2016-3370] "The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka ""PDF Library Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3374."  
  
[CVE-2016-3371] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain sensitive information via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3372] "The kernel API in Microsoft Windows Vista SP2 and Windows Server 2008 SP2 does not properly enforce permissions, which allows local users to spoof processes, spoof inter-process communication, or cause a denial of service via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3373] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 does not properly implement registry access control, which allows local users to obtain sensitive account information via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-3374] "The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka ""PDF Library Information Disclosure Vulnerability,"" a different vulnerability than CVE-2016-3370."  
  
[CVE-2016-3375] "The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Scripting Engine Memory Corruption Vulnerability."""  
  
[CVE-2016-3376] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-7185, and CVE-2016-7211."  
  
[CVE-2016-3393] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-3396] "Graphics Device Interface (aka GDI or GDI+) in Microsoft Windows Vista SP2  
[CVE-2016-5063] The RSCD agent in BMC Server Automation before 8.6 SP1 Patch 2 and 8.7 before Patch 3 on Windows might allow remote attackers to bypass authorization checks and make an RPC call via unspecified vectors.  
  
[CVE-2016-6848] "An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. API requests can be used to inject, generate and download executable files to the client (""Reflected File Download""). Malicious platform specific (e.g. Microsoft Windows) batch file can be created via a trusted domain without authentication that, if executed by the user, may lead to local code execution."  
  
[CVE-2016-7165] "A vulnerability has been identified in Primary Setup Tool (PST) (All versions < V4.2 HF1), SIMATIC IT Production Suite (All versions < V7.0 SP1 HFX 2), SIMATIC NET PC-Software (All versions < V14), SIMATIC PCS 7 V7.1 (All versions), SIMATIC PCS 7 V8.0 (All versions), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions < V8.2 SP1), SIMATIC STEP 7 (TIA Portal) V13 (All versions < V13 SP2), SIMATIC STEP 7 V5.X (All versions < V5.5 SP4 HF11), SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced (All versions < V14), SIMATIC WinCC (TIA Portal) Professional V13 (All versions < V13 SP2), SIMATIC WinCC (TIA Portal) Professional V14 (All versions < V14 SP1), SIMATIC WinCC Runtime Professional V13 (All versions < V13 SP2), SIMATIC WinCC Runtime Professional V14 (All versions < V14 SP1), SIMATIC WinCC V7.0 SP2 and earlier versions (All versions < V7.0 SP2 Upd 12), SIMATIC WinCC V7.0 SP3 (All versions < V7.0 SP3 Upd 8), SIMATIC WinCC V7.2 (All versions < V7.2 Upd 14), SIMATIC WinCC V7.3 (All versions < V7.3 Upd 11), SIMATIC WinCC V7.4 (All versions < V7.4 SP1), SIMIT V9.0 (All versions < V9.0 SP1), SINEMA Remote Connect Client (All versions < V1.0 SP3), SINEMA Server (All versions < V13 SP2), SOFTNET Security Client V5.0 (All versions), Security Configuration Tool (SCT) (All versions < V4.3 HF1), TeleControl Server Basic (All versions < V3.0 SP2), WinAC RTX 2010 SP2 (All versions), WinAC RTX F 2010 SP2 (All versions). Unquoted service paths could allow local Microsoft Windows operating system users to escalate their privileges if the affected products are not installed under their default path (""C:\Program Files\\*"" or the localized equivalent)."  
  
[CVE-2016-7182] "The Graphics component in Microsoft Windows Vista SP2  
[CVE-2016-7184] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Windows Common Log File System Driver Elevation of Privilege Vulnerability,"" a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-3343."  
  
[CVE-2016-7185] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7211."  
  
[CVE-2016-7188] "The Standard Collector Service in Windows Diagnostics Hub in Microsoft Windows 10 Gold, 1511, and 1607 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Diagnostics Hub Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7205] "Animation Manager in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Animation Manager Memory Corruption Vulnerability."""  
  
[CVE-2016-7210] "atmfd.dll in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted Open Type font on a web site, aka ""Open Type Font Information Disclosure Vulnerability."""  
  
[CVE-2016-7211] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7185."  
  
[CVE-2016-7212] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow remote attackers to execute arbitrary code via a crafted image file, aka ""Windows Remote Code Execution Vulnerability."""  
  
[CVE-2016-7214] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to bypass the ASLR protection mechanism via a crafted application, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2016-7215] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7216] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandles permissions, which allows local users to gain privileges via a crafted application, aka ""Windows Kernel Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7217] "Media Foundation in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Media Foundation Memory Corruption Vulnerability."""  
  
[CVE-2016-7218] "Bowser.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Windows Bowser.sys Information Disclosure Vulnerability."""  
  
[CVE-2016-7219] "The Crypto driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Windows Crypto Driver Information Disclosure Vulnerability."""  
  
[CVE-2016-7220] "Virtual Secure Mode in Microsoft Windows 10 allows local users to obtain sensitive information via a crafted application, aka ""Virtual Secure Mode Information Disclosure Vulnerability."""  
  
[CVE-2016-7221] "Input Method Editor (IME) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles DLL loading, which allows local users to gain privileges via unspecified vectors, aka ""Windows IME Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7222] "Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a crafted UNC pathname in a task, aka ""Task Scheduler Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7223] "Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka ""VHD Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7224] "Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka ""VHD Driver Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7237] "Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote authenticated users to cause a denial of service (system hang) via a crafted request, aka ""Local Security Authority Subsystem Service Denial of Service Vulnerability."""  
  
[CVE-2016-7238] "Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandle caching for NTLM password-change requests, which allows local users to gain privileges via a crafted application, aka ""Windows NTLM Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7246] "The kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7247] "Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow physically proximate attackers to bypass the Secure Boot protection mechanism via a crafted boot policy, aka ""Secure Boot Component Vulnerability."""  
  
[CVE-2016-7248] "Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka ""Microsoft Video Control Remote Code Execution Vulnerability."""  
  
[CVE-2016-7255] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7256] "atmfd.dll in the Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Open Type Font Remote Code Execution Vulnerability."""  
  
[CVE-2016-7257] "The GDI component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office for Mac 2011, and Office 2016 for Mac allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2016-7258] "The kernel in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 mishandles page-fault system calls, which allows local users to obtain sensitive information from arbitrary processes via a crafted application, aka ""Windows Kernel Memory Address Information Disclosure Vulnerability."""  
  
[CVE-2016-7259] "The Graphics Component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7260] "The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7271] "The Secure Kernel Mode implementation in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to bypass the virtual trust level (VTL) protection mechanism via a crafted application, aka ""Secure Kernel Mode Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7272] "The Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Graphics Remote Code Execution Vulnerability."""  
  
[CVE-2016-7273] "The Graphics component in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Graphics Remote Code Execution Vulnerability."""  
  
[CVE-2016-7274] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."""  
  
[CVE-2016-7278] "Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Windows Hyperlink Object Library Information Disclosure Vulnerability."""  
  
[CVE-2016-7292] "The Installer in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ""Windows Installer Elevation of Privilege Vulnerability."""  
  
[CVE-2016-7295] "The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information from process memory via a crafted application, aka ""Windows Common Log File System Driver Information Disclosure Vulnerability."""  
  
[CVE-2016-9192] A vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and execute an arbitrary executable file with privileges equivalent to the Microsoft Windows operating system SYSTEM account. More Information: CSCvb68043. Known Affected Releases: 4.3(2039) 4.3(748). Known Fixed Releases: 4.3(4019) 4.4(225).  
  
[CVE-2016-9459] Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a log pollution vulnerability potentially leading to a local XSS. The download log functionality in the admin screen is delivering the log in JSON format to the end-user. The file was delivered with an attachment disposition forcing the browser to download the document. However, Firefox running on Microsoft Windows would offer the user to open the data in the browser as an HTML document. Thus any injected data in the log would be executed.  
  
[CVE-2017-0001] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0004] "The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to cause a denial of service (reboot) via a crafted authentication request, aka ""Local Security Authority Subsystem Service Denial of Service Vulnerability."""  
  
[CVE-2017-0005] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0007] "Device Guard in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows remote attackers to modify PowerShell script without invalidating associated signatures, aka ""PowerShell Security Feature Bypass Vulnerability."""  
  
[CVE-2017-0014] "The Windows Graphics Component in Microsoft Office 2010 SP2  
[CVE-2017-0016] "Microsoft Windows 10 Gold, 1511, and 1607  
[CVE-2017-0021] "Hyper-V in Microsoft Windows 10 1607 and Windows Server 2016 does not properly validate vSMB packet data, which allows attackers to execute arbitrary code on a target OS, aka ""Hyper-V System Data Structure Vulnerability."" This vulnerability is different from that described in CVE-2017-0095."  
  
[CVE-2017-0022] "Microsoft XML Core Services (MSXML) in Windows 10 Gold, 1511, and 1607  
[CVE-2017-0024] "The kernel-mode drivers in Microsoft Windows 10 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0025] "The kernel-mode drivers in Microsoft Windows Vista  
[CVE-2017-0026] "The kernel-mode drivers in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0038] gdi32.dll in Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information from process heap memory via a crafted EMF file, as demonstrated by an EMR\_SETDIBITSTODEVICE record with modified Device Independent Bitmap (DIB) dimensions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-3216, CVE-2016-3219, and/or CVE-2016-3220.  
  
[CVE-2017-0039] "Microsoft Windows Vista SP2 and Server 2008 SP2 mishandle dynamic link library (DLL) loading, which allows local users to gain privileges via a crafted application, aka ""Library Loading Input Validation Remote Code Execution Vulnerability."""  
  
[CVE-2017-0042] "Windows Media Player in Microsoft Windows 8.1  
[CVE-2017-0043] "Active Directory Federation Services in Microsoft Windows 10 1607, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka ""Microsoft Active Directory Federation Services Information Disclosure Vulnerability."""  
  
[CVE-2017-0047] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0050] "The kernel API in Microsoft Windows Vista SP2  
[CVE-2017-0051] "Microsoft Windows 10 1607 and Windows Server 2016 allow remote attackers to cause a denial of service (application hang) via a crafted Office document, aka ""Microsoft Hyper-V Network Switch Denial of Service Vulnerability."" This vulnerability is different from those described in CVE-2017-0074, CVE-2017-0076, CVE-2017-0097, CVE-2017-0098, and CVE-2017-0099."  
  
[CVE-2017-0055] "Microsoft Internet Information Server (IIS) in Windows Vista SP2  
[CVE-2017-0056] "The kernel-mode drivers in Microsoft Windows Vista SP2  
[CVE-2017-0057] "DNS client in Microsoft Windows 8.1  
[CVE-2017-0058] "A Win32k information disclosure vulnerability exists in Microsoft Windows when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system, aka ""Win32k Information Disclosure Vulnerability."""  
  
[CVE-2017-0060] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0061] "The Color Management Module (ICM32.dll) memory handling functionality in Windows Vista SP2, Windows Server 2008 SP2 and R2, and Windows 7 SP1 allows remote attackers to bypass ASLR and execute code in combination with another vulnerability through a crafted website, aka ""Microsoft Color Management Information Disclosure Vulnerability."" This vulnerability is different from that described in CVE-2017-0063."  
  
[CVE-2017-0062] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0066] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0135 and CVE-2017-0140."  
  
[CVE-2017-0072] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0073] "The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2  
[CVE-2017-0074] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0075] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0076] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0078] "The kernel-mode drivers in Microsoft Windows 8.1  
[CVE-2017-0080] "The kernel-mode drivers in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0081, and CVE-2017-0082."  
  
[CVE-2017-0081] "The kernel-mode drivers in Microsoft Windows 8.1  
[CVE-2017-0082] "The kernel-mode drivers in Microsoft Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."" This vulnerability is different from those described in CVE-2017-0024, CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, and CVE-2017-0081."  
  
[CVE-2017-0083] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0084] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0085] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0086] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0087] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090."  
  
[CVE-2017-0088] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Windows Uniscribe Remote Code Execution Vulnerability."""  
  
[CVE-2017-0089] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0090."  
  
[CVE-2017-0090] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka ""Uniscribe Remote Code Execution Vulnerability."" This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0089."  
  
[CVE-2017-0091] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0092] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0095] "Hyper-V in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 does not properly validate vSMB packet data, which allows attackers to execute arbitrary code on a target OS, aka ""Hyper-V vSMB Remote Code Execution Vulnerability."" This vulnerability is different from that described in CVE-2017-0021."  
  
[CVE-2017-0096] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0097] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0098] "Hyper-V in Microsoft Windows 10 Gold, 1511, and 1607  
[CVE-2017-0099] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0100] "A DCOM object in Helppane.exe in Microsoft Windows 7 SP1  
[CVE-2017-0101] "The kernel-mode drivers in Transaction Manager in Microsoft Windows Vista SP2  
[CVE-2017-0102] "Microsoft Windows Vista SP2  
[CVE-2017-0103] "The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows Server 2012 mishandles registry objects in memory, which allows local users to gain privileges via a crafted application, aka ""Windows Registry Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0104] "The iSNS Server service in Microsoft Windows Server 2008 SP2 and R2, Windows Server 2012 Gold and R2, and Windows Server 2016 allows remote attackers to issue malicious requests via an integer overflow, aka ""iSNS Server Memory Corruption Vulnerability."""  
  
[CVE-2017-0108] "The Windows Graphics Component in Microsoft Office 2007 SP3  
[CVE-2017-0109] "Hyper-V in Microsoft Windows Vista SP2  
[CVE-2017-0111] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0112] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0113] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0114] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0115] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0116] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0117] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0118] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0119] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0120] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Windows Uniscribe Information Disclosure Vulnerability."""  
  
[CVE-2017-0121] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0122] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0123] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0124] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0125] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0126] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0127, and CVE-2017-0128."  
  
[CVE-2017-0127] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, and CVE-2017-0128."  
  
[CVE-2017-0128] "Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""Uniscribe Information Disclosure Vulnerability."" CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, and CVE-2017-0127."  
  
[CVE-2017-0135] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0140."  
  
[CVE-2017-0140] "Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability."" This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0135."  
  
[CVE-2017-0143] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0144] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0145] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0146] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0147] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0148] "The SMBv1 server in Microsoft Windows Vista SP2  
[CVE-2017-0154] "Microsoft Internet Explorer 11 on Windows 10, 1511, and 1606 and Windows Server 2016 does not enforce cross-domain policies, allowing attackers to access information from one domain and inject it into another via a crafted application, aka, ""Internet Explorer Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0155] "The Graphics component in the kernel in Microsoft Windows Vista SP2  
[CVE-2017-0156] "An elevation of privilege vulnerability exists in Windows 7, Windows 8.1, Windows RT 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 when the Microsoft Graphics Component fails to properly handle objects in memory, aka ""Windows Graphics Component Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0158] "An elevation of privilege vulnerability exists when Microsoft Windows running on Windows 10, Windows 10 1511, Windows 8.1 Windows RT 8.1, and Windows Server 2012 R2 fails to properly sanitize handles in memory, aka ""Scripting Engine Memory Corruption Vulnerability."""  
  
[CVE-2017-0161] "The Windows NetBT Session Services component on Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to maintain certain sequencing requirements, aka ""NetBIOS Remote Code Execution Vulnerability""."  
  
[CVE-2017-0165] "An elevation of privilege vulnerability exists when Microsoft Windows running on Windows 10, Windows 10 1511, Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 fails to properly sanitize handles in memory, aka ""Windows Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0171] "Windows DNS Server allows a denial of service vulnerability when Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 are configured to answer version queries, aka ""Windows DNS Server Denial of Service Vulnerability""."  
  
[CVE-2017-0173] "Microsoft Windows 10 1607 and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0215, CVE-2017-0216, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0176] A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.  
  
[CVE-2017-0178] "A denial of service vulnerability exists when Microsoft Hyper-V running on Windows 10, Windows 10 1511, Windows 10 1607, Windows 8.1, Windows Server 2012 R2, and Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0179] "A denial of service vulnerability exists when Microsoft Hyper-V running on a Windows 10, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0182] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0183, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0183] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0184, CVE-2017-0185, and CVE-2017-0186."  
  
[CVE-2017-0185] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, and CVE-2017-0186."  
  
[CVE-2017-0186] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch running on a Windows 10, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from a privileged user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability."" This CVE ID is unique from CVE-2017-0178, CVE-2017-0179, CVE-2017-0182, CVE-2017-0183, CVE-2017-0184, and CVE-2017-0185."  
  
[CVE-2017-0190] "The GDI component in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka ""GDI Information Disclosure Vulnerability."""  
  
[CVE-2017-0192] "The Adobe Type Manager Font Driver (ATMFD.dll) in Microsoft Windows Vista SP2  
[CVE-2017-0193] "Windows Hyper-V in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to gain elevated privileges on a target guest operating system when Windows Hyper-V instruction emulation fails to properly enforce privilege levels, aka ""Hypervisor Code Integrity Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0199] "Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka ""Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."""  
  
[CVE-2017-0211] "An elevation of privilege vulnerability exists in Windows 10, Windows 8.1, Windows RT 8.1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 versions of Microsoft Windows OLE when it fails an integrity-level check, aka ""Windows OLE Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0212] "Windows Hyper-V allows an elevation of privilege vulnerability when Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 fail to properly validate vSMB packet data, aka ""Windows Hyper-V vSMB Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0213] "Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka ""Windows COM Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-0214."  
  
[CVE-2017-0214] "Windows COM in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when Windows fails to properly validate input before loading type libraries, aka ""Windows COM Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-0213."  
  
[CVE-2017-0215] "Microsoft Windows 10 1607 and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0216, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0216] "Microsoft Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0218, and CVE-2017-0219."  
  
[CVE-2017-0218] "Microsoft Windows 10 Gold, Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0216, and CVE-2017-0219."  
  
[CVE-2017-0219] "Microsoft Windows 10 Gold, Windows 10 1511, Windows 10 1607, and Windows Server 2016 allow an attacker to exploit a security feature bypass vulnerability in Device Guard that could allow the attacker to inject malicious code into a Windows PowerShell session, aka ""Device Guard Code Integrity Policy Security Feature Bypass Vulnerability."" This CVE ID is unique from CVE-2017-0173, CVE-2017-0215, CVE-2017-0216, and CVE-2017-0218."  
  
[CVE-2017-0250] "Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to buffer overflow, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-0258] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-0175, CVE-2017-0220, and CVE-2017-0259."  
  
[CVE-2017-0259] "The Windows kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-0175, CVE-2017-0220, and CVE-2017-0258."  
  
[CVE-2017-0263] "The kernel-mode drivers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka ""Win32k Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0267] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0268] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0269] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0273 and CVE-2017-0280."  
  
[CVE-2017-0270] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0271] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0274, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0272] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0277, CVE-2017-0278, and CVE-2017-0279."  
  
[CVE-2017-0273] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0269 and CVE-2017-0280."  
  
[CVE-2017-0274] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0275, and CVE-2017-0276."  
  
[CVE-2017-0275] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, and CVE-2017-0276."  
  
[CVE-2017-0276] "Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, and CVE-2017-0275."  
  
[CVE-2017-0277] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0278, and CVE-2017-0279."  
  
[CVE-2017-0278] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0277, and CVE-2017-0279."  
  
[CVE-2017-0279] "The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka ""Windows SMB Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0272, CVE-2017-0277, and CVE-2017-0278."  
  
[CVE-2017-0280] "The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability"". This CVE ID is unique from CVE-2017-0269 and CVE-2017-0273."  
  
[CVE-2017-0282] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0284, CVE-2017-0285, and CVE-2017-8534."  
  
[CVE-2017-0283] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office Word Viewer, Microsoft Lync 2013 SP1, Skype for Business 2016, Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows, and Microsoft Silverlight 5 when installed on Microsoft Windows allows a remote code execution vulnerability due to the way it handles objects in memory, aka ""Windows Uniscribe Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8528."  
  
[CVE-2017-0284] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0285, and CVE-2017-8534."  
  
[CVE-2017-0285] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, and Microsoft Office Word Viewer allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0284, and CVE-2017-8534."  
  
[CVE-2017-0290] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 does not properly scan a specially crafted file leading to memory corruption, aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability."""  
  
[CVE-2017-0293] "Microsoft Windows PDF Library in Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability when it improperly handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability""."  
  
[CVE-2017-0294] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute remote code when Windows fails to properly handle cabinet files, aka ""Windows Remote Code Execution Vulnerability""."  
  
[CVE-2017-0295] "Microsoft Windows 10 1607 and 1703, and Windows Server 2016 allow an authenticated attacker to modify the C:\Users\DEFAULT folder structure, aka ""Windows Default Folder Tampering Vulnerability""."  
  
[CVE-2017-0296] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to elevate privilege when tdx.sys fails to check the length of a buffer prior to copying memory to it, aka ""Windows TDX Elevation of Privilege Vulnerability""."  
  
[CVE-2017-0297] "The kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0299, CVE-2017-0300."  
  
[CVE-2017-0298] "A DCOM object in Helppane.exe in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016, when configured to run as the interactive user, allows an authenticated attacker to run arbitrary code in another user's session, aka ""Windows COM Session Elevation of Privilege Vulnerability."""  
  
[CVE-2017-0299] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, and CVE-2017-0297."  
  
[CVE-2017-0300] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-10769] "XnView Classic for Windows Version 2.40 might allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .rle file, related to ""Data from Faulting Address controls Branch Selection starting at ntdll\_77df0000!memcmp+0x0000000000000018"" (without RPC initialization)."  
  
[CVE-2017-10772] "XnView Classic for Windows Version 2.40 might allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .rle file, related to ""Data from Faulting Address controls Branch Selection starting at ntdll\_77df0000!memcmp+0x0000000000000018"" (with RPC initialization)."  
  
[CVE-2017-11762] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-11763."  
  
[CVE-2017-11763] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-11763."  
  
[CVE-2017-11764] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-8756."  
  
[CVE-2017-11765] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11784, CVE-2017-11785, and CVE-2017-11814."  
  
[CVE-2017-11766] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-8751."  
  
[CVE-2017-11769] "The Microsoft Windows TRIE component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way it handles loading dll files, aka ""TRIE Remote Code Execution Vulnerability""."  
  
[CVE-2017-11771] "The Microsoft Windows Search component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly handle DNS responses, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-11772] "The Microsoft Windows Search component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure when it fails to properly handle objects in memory, aka ""Microsoft Search Information Disclosure Vulnerability""."  
  
[CVE-2017-11779] "The Microsoft Windows Domain Name System (DNS) DNSAPI.dll on Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly handle DNS responses, aka ""Windows DNSAPI Remote Code Execution Vulnerability""."  
  
[CVE-2017-11780] "The Server Message Block 1.0 (SMBv1) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a remote code execution vulnerability when it fails to properly handle certain requests, aka ""Windows SMB Remote Code Execution Vulnerability""."  
  
[CVE-2017-11781] "The Microsoft Server Block Message (SMB) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a denial of service vulnerability when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability""."  
  
[CVE-2017-11782] "The Microsoft Server Block Message (SMB) on Microsoft Windows 10 1607 and Windows Server 2016, allows an elevation of privilege vulnerability when an attacker sends specially crafted requests to the server, aka ""Windows SMB Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11783] "Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability in the way it handles calls to Advanced Local Procedure Call (ALPC), aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11784] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11785, and CVE-2017-11814."  
  
[CVE-2017-11785] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11784, and CVE-2017-11814."  
  
[CVE-2017-11790] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2017-11791] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11834."  
  
[CVE-2017-11792] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allow an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11793, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11793] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11794] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8726 and CVE-2017-11803."  
  
[CVE-2017-11796] "ChakraCore and Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11798] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11799] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11800] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11802] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11803] "Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11833 and CVE-2017-11844."  
  
[CVE-2017-11804] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11805] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11806] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11807] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11808] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11809] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11810, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11810] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11811, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11811] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11812] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11812, and CVE-2017-11821."  
  
[CVE-2017-11813] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11822."  
  
[CVE-2017-11814] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11765, CVE-2017-11784, and CVE-2017-11785."  
  
[CVE-2017-11815] "The Microsoft Server Block Message (SMB) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability in the way that it handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability""."  
  
[CVE-2017-11816] "The Microsoft Windows Graphics Device Interface (GDI) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability in the way it handles objects in memory, aka ""Windows GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-11817] "The Microsoft Windows Kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an information disclosure vulnerability when it improperly validates objects in memory, aka ""Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-11818] "The Microsoft Windows Storage component on Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass vulnerability when it fails to validate an integrity-level check, aka ""Windows Storage Security Feature Bypass Vulnerability""."  
  
[CVE-2017-11819] "Microsoft Windows 7 SP1 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft browsers handle objects in memory, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2017-11821] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11792, CVE-2017-11793, CVE-2017-11796, CVE-2017-11797, CVE-2017-11798, CVE-2017-11799, CVE-2017-11800, CVE-2017-11801, CVE-2017-11802, CVE-2017-11804, CVE-2017-11805, CVE-2017-11806, CVE-2017-11807, CVE-2017-11808, CVE-2017-11809, CVE-2017-11810, CVE-2017-11811, and CVE-2017-11812."  
  
[CVE-2017-11822] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11813."  
  
[CVE-2017-11823] "The Microsoft Device Guard on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass by the way it handles Windows PowerShell sessions, aka ""Microsoft Windows Security Feature Bypass""."  
  
[CVE-2017-11824] "The Microsoft Graphics Component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability in the way it handles objects in memory, aka ""Windows Graphics Component Elevation of Privilege Vulnerability""."  
  
[CVE-2017-11827] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability""."  
  
[CVE-2017-11829] Microsoft Windows 10 allows an elevation of privilege vulnerability when the Windows Update Delivery Optimization does not properly enforce file share permissions.  
  
[CVE-2017-11832] "The Microsoft Windows embedded OpenType (EOT) font engine in Windows 7 SP1, Windows Server 2008 SP2 and 2008 R2 SP1, and Windows Server 2012 allows an attacker to potentially read data that was not intended to be disclosed, due to the way that the Microsoft Windows EOT font engine parses specially crafted embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability."" This CVE ID is unique from CVE-2017-11835."  
  
[CVE-2017-11833] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to determine the origin of all webpages in the affected browser, due to how Microsoft Edge handles cross-origin requests, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11844."  
  
[CVE-2017-11834] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11791."  
  
[CVE-2017-11835] "Microsoft graphics in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an attacker to potentially read data that was not intended to be disclosed due to the way that the Microsoft Windows Embedded OpenType (EOT) font engine parses specially crafted embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11832."  
  
[CVE-2017-11836] "ChakraCore, and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11837] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11838] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11839] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to take control of an affected system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11840] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11841] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11843] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11844] "Microsoft Edge in Microsoft Windows 10 1703, 1709 and Windows Server, version 1709 allows an attacker to obtain information to further compromise the user's system, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11803 and CVE-2017-11833."  
  
[CVE-2017-11845] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-11846] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11848] "Internet Explorer in Microsoft Microsoft Windows 7 SP1, Windows Server 2008 SP2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to detect the navigation of the user leaving a maliciously crafted page, due to how page content is handled by Internet Explorer, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2017-11850] "Microsoft Graphics Component in Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to log on to an affected system and run a specially crafted application due to improper handling of objects in memory, aka ""Microsoft Graphics Component Information Disclosure Vulnerability""."  
  
[CVE-2017-11852] "Microsoft GDI Component in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an attacker to log on to an affected system and run a specially crafted application to compromise the user's system, due improperly disclosing kernel memory addresses, aka ""Windows GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-11855] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11856."  
  
[CVE-2017-11856] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11855."  
  
[CVE-2017-11858] "ChakraCore and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11861] "Microsoft Edge in Windows 10 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11862] "ChakraCore and Microsoft Edge in Windows 10 1709 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11863] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to trick a user into loading a page containing malicious content, due to how the Edge Content Security Policy (CSP) validates documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11872 and CVE-2017-11874."  
  
[CVE-2017-11866] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11869] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how Microsoft browsers handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11870, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11870] "ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11871, and CVE-2017-11873."  
  
[CVE-2017-11871] "ChakraCore and Microsoft Edge in Windows 10 1703, 1709, and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11873."  
  
[CVE-2017-11872] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to force the browser to send data that would otherwise be restricted to a destination website of the attacker's choice, due to how Microsoft Edge handles redirect requests, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11874."  
  
[CVE-2017-11873] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11859, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, and CVE-2017-11871."  
  
[CVE-2017-11874] "Microsoft Edge in Microsoft Windows 10 1703, 1709, Windows Server, version 1709, and ChakraCore allows an attacker to bypass Control Flow Guard (CFG) to run arbitrary code on a target system, due to how Microsoft Edge handles accessing memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-11863 and CVE-2017-11872."  
  
[CVE-2017-11886] "Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11887] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handle objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11906 and CVE-2017-11919."  
  
[CVE-2017-11888] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-11889] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11890] "Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11893] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11894] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and and Internet Explorer adn Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11895] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11899] "Device Guard in Windows 10 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows a security feature bypass vulnerability due to the way untrusted files are handled, aka ""Microsoft Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-11901] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11903] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11905] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11906] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11919."  
  
[CVE-2017-11907] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11912] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11913] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11914] "ChakraCore and Microsoft Edge in Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930."  
  
[CVE-2017-11918] "ChakraCore and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to gain the same user rights as the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, and CVE-2017-11930."  
  
[CVE-2017-11919] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016, and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-11887 and CVE-2017-11906."  
  
[CVE-2017-11927] "Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allow an information vulnerability due to the way the Windows its:// protocol handler determines the zone of a request, aka ""Microsoft Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-11930] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11890, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, and CVE-2017-11916."  
  
[CVE-2017-11937] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, 1709 and Windows Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to remote code execution. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-11940] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, 1709 and Windows Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to remote code execution. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"". This is different than CVE-2017-11937."  
  
[CVE-2017-12266] A vulnerability in the routine that loads DLL files in Cisco Meeting App for Windows could allow an authenticated, local attacker to run an executable file with privileges equivalent to those of Cisco Meeting App. The vulnerability is due to incomplete input validation of the path name for DLL files before they are loaded. An attacker could exploit this vulnerability by installing a crafted DLL file in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to those of Cisco Meeting App. The attacker would need valid user credentials to exploit this vulnerability. Cisco Bug IDs: CSCvd77907.  
  
[CVE-2017-12312] An untrusted search path (aka DLL Preloading) vulnerability in the Cisco Immunet antimalware installer could allow an authenticated, local attacker to execute arbitrary code via DLL hijacking if a local user with administrative privileges executes the installer in the current working directory where a crafted DLL has been placed by an attacker. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. An attacker would need valid user credentials to exploit this vulnerability. Cisco Bug IDs: CSCvf23928.  
  
[CVE-2017-12313] An untrusted search path (aka DLL Preload) vulnerability in the Cisco Network Academy Packet Tracer software could allow an authenticated, local attacker to execute arbitrary code via DLL hijacking if a local user with administrative privileges executes the installer in the current working directory where a crafted DLL has been placed by an attacker. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. An attacker would need valid user credentials to exploit this vulnerability.  
  
[CVE-2017-16744] A path traversal vulnerability in Tridium Niagara AX Versions 3.8 and prior and Niagara 4 systems Versions 4.4 and prior installed on Microsoft Windows Systems can be exploited by leveraging valid platform (administrator) credentials.  
  
[CVE-2017-3222] Hard-coded credentials in AmosConnect 8 allow remote attackers to gain full administrative privileges, including the ability to execute commands on the Microsoft Windows host platform with SYSTEM privileges by abusing AmosConnect Task Manager.  
  
[CVE-2017-3823] An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.  
  
[CVE-2017-4028] Maliciously misconfigured registry vulnerability in all Microsoft Windows products in McAfee consumer and corporate products allows an administrator to inject arbitrary code into a debugged McAfee process via manipulation of registry parameters.  
  
[CVE-2017-6638] A vulnerability in how DLL files are loaded with Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and run an executable file with privileges equivalent to the Microsoft Windows SYSTEM account. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with privileges equivalent to the SYSTEM account. The attacker would need valid user credentials to exploit this vulnerability. This vulnerability affects all Cisco AnyConnect Secure Mobility Client for Windows software versions prior to 4.4.02034. Cisco Bug IDs: CSCvc97928.  
  
[CVE-2017-6639] A vulnerability in the role-based access control (RBAC) functionality of Cisco Prime Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to access sensitive information or execute arbitrary code with root privileges on an affected system. The vulnerability is due to the lack of authentication and authorization mechanisms for a debugging tool that was inadvertently enabled in the affected software. An attacker could exploit this vulnerability by remotely connecting to the debugging tool via TCP. A successful exploit could allow the attacker to access sensitive information about the affected software or execute arbitrary code with root privileges on the affected system. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM) Software Releases 10.1(1) and 10.1(2) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd09961.  
  
[CVE-2017-6640] A vulnerability in Cisco Prime Data Center Network Manager (DCNM) Software could allow an unauthenticated, remote attacker to log in to the administrative console of a DCNM server by using an account that has a default, static password. The account could be granted root- or system-level privileges. The vulnerability exists because the affected software has a default user account that has a default, static password. The user account is created automatically when the software is installed. An attacker could exploit this vulnerability by connecting remotely to an affected system and logging in to the affected software by using the credentials for this default user account. A successful exploit could allow the attacker to use this default user account to log in to the affected software and gain access to the administrative console of a DCNM server. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM) Software releases prior to Release 10.2(1) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd95346.  
  
[CVE-2017-6753] A vulnerability in Cisco WebEx browser extensions for Google Chrome and Mozilla Firefox could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server, Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center), and Cisco WebEx Meetings when they are running on Microsoft Windows. The vulnerability is due to a design defect in the extension. An attacker who can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser. The following versions of the Cisco WebEx browser extensions are affected: Versions prior to 1.0.12 of the Cisco WebEx extension on Google Chrome, Versions prior to 1.0.12 of the Cisco WebEx extension on Mozilla Firefox. Cisco Bug IDs: CSCvf15012 CSCvf15020 CSCvf15030 CSCvf15033 CSCvf15036 CSCvf15037.  
  
[CVE-2017-7269] "Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with ""If: <http://"" in a PROPFIND request, as exploited in the wild in July or August 2016."  
  
[CVE-2017-8461] "Windows RPC with Routing and Remote Access enabled in Windows XP and Windows Server 2003 allows an attacker to execute code on a targeted RPC server which has Routing and Remote Access enabled via a specially crafted application, aka ""Windows RPC Remote Code Execution Vulnerability."""  
  
[CVE-2017-8462] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8464] "Windows Shell in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows local users or remote attackers to execute arbitrary code via a crafted .LNK file, which is not properly handled during icon display in Windows Explorer or any other application that parses the icon of the shortcut. aka ""LNK Remote Code Execution Vulnerability."""  
  
[CVE-2017-8465] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to run processes in an elevated context when the Windows kernel improperly handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability."" This CVE ID is unique from CVE-2017-8468."  
  
[CVE-2017-8467] "Graphics in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8468] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to run processes in an elevated context when the Windows kernel improperly handles objects in memory, aka ""Win32k Elevation of Privilege Vulnerability."" This CVE ID is unique from CVE-2017-8465."  
  
[CVE-2017-8469] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8470] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8471] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8472] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, and Windows Server 2012 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8473, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8473] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8475, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8474] "The kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8476, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8475] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8477, and CVE-2017-8484."  
  
[CVE-2017-8476] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8478, CVE-2017-8479, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8477] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, and CVE-2017-8484."  
  
[CVE-2017-8478] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8480, CVE-2017-8479, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8479] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8481, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8480] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8481] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8482] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8483] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8484] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an authenticated attacker to run a specially crafted application when the Windows kernel improperly initializes objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8470, CVE-2017-8471, CVE-2017-8472, CVE-2017-8473, CVE-2017-8475, and CVE-2017-8477."  
  
[CVE-2017-8485] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8486] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an information disclosure due to the way it handles objects in memory, aka ""Win32k Information Disclosure Vulnerability""."  
  
[CVE-2017-8488] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8489] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8490, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8490] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8491, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8491] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8492, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8492] "The kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application. aka ""Windows Kernel Information Disclosure Vulnerability,"" a different vulnerability than CVE-2017-8491, CVE-2017-8490, CVE-2017-8489, CVE-2017-8488, CVE-2017-8485, CVE-2017-8483, CVE-2017-8482, CVE-2017-8480, CVE-2017-8479, CVE-2017-8478, CVE-2017-8476, CVE-2017-8474, CVE-2017-8469, CVE-2017-8462, CVE-2017-0300, CVE-2017-0299, and CVE-2017-0297."  
  
[CVE-2017-8493] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to set variables that are either read-only or require authentication when Windows fails to enforce case sensitivity for certain variable checks, aka ""Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8494] "Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a locally-authenticated attacker to run a specially crafted application on a targeted system when Windows Secure Kernel Mode fails to properly handle objects in memory, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8495] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to bypass Extended Protection for Authentication when Kerberos fails to prevent tampering with the SNAME field during ticket exchange, aka ""Kerberos SNAME Security Feature Bypass Vulnerability"" or Orpheus' Lyre."  
  
[CVE-2017-8496] "Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8497."  
  
[CVE-2017-8497] "Microsoft Edge in Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user when Microsoft Edge improperly accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8496."  
  
[CVE-2017-8498] "Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read data not intended to be disclosed when Edge allows JavaScript XML DOM objects to detect installed browser extensions, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8504."  
  
[CVE-2017-8499] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8520, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8503] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to escape from the AppContainer sandbox, aka ""Microsoft Edge Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8642."  
  
[CVE-2017-8504] "Microsoft Edge in Windows 10 1607 and 1703, and Windows Server 2016 allows an attacker to read the URL of a cross-origin request when the Microsoft Edge Fetch API incorrectly handles a filtered response type, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8498."  
  
[CVE-2017-8515] "Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an unauthenticated attacker to send a specially crafted kernel mode request to cause a denial of service on the target system, aka ""Windows VAD Cloning Denial of Service Vulnerability""."  
  
[CVE-2017-8517] "Microsoft browsers in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8522 and CVE-2017-8524."  
  
[CVE-2017-8519] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8547."  
  
[CVE-2017-8520] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8521, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8521] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the Edge JavaScript scripting engine fails to handle objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8548, and CVE-2017-8549."  
  
[CVE-2017-8522] "Microsoft browsers in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8517 and CVE-2017-8524."  
  
[CVE-2017-8523] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge fails to correctly apply Same Origin Policy for HTML elements present in other browser windows, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8530 and CVE-2017-8555."  
  
[CVE-2017-8524] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8517 and CVE-2017-8522."  
  
[CVE-2017-8528] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows a remote code execution vulnerability due to the way it handles objects in memory, aka ""Windows Uniscribe Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-0283."  
  
[CVE-2017-8529] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to detect specific files on the user's computer when affected Microsoft scripting engines do not properly handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2017-8530] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when Microsoft Edge does not properly enforce same-origin policies, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8555."  
  
[CVE-2017-8531] "Graphics in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016, Microsoft Office 2007 Service Pack 3, and Microsoft Office 2010 Service Pack 2 allows improper disclosure of memory contents, aka ""Graphics Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0286, CVE-2017-0287, CVE-2017-0288, CVE-2017-0289, CVE-2017-8532, and CVE-2017-8533."  
  
[CVE-2017-8534] "Uniscribe in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, Windows Server 2016, Microsoft Office 2007 SP3, and Microsoft Office 2010 SP2 allows improper disclosure of memory contents, aka ""Windows Uniscribe Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-0282, CVE-2017-0284, and CVE-2017-0285."  
  
[CVE-2017-8535] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8536, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8536] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8537] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8539, and CVE-2017-8542."  
  
[CVE-2017-8538] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8540 and CVE-2017-8541."  
  
[CVE-2017-8539] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8542."  
  
[CVE-2017-8540] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8538 and CVE-2017-8541."  
  
[CVE-2017-8541] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability"", a different vulnerability than CVE-2017-8538 and CVE-2017-8540."  
  
[CVE-2017-8542] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka ""Microsoft Malware Protection Engine Denial of Service Vulnerability"", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8539."  
  
[CVE-2017-8543] "Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to take control of the affected system when Windows Search fails to handle objects in memory, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-8544] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to obtain information to further compromise the user's system when Windows Search fails to handle objects in memory, aka ""Windows Search Information Disclosure Vulnerability""."  
  
[CVE-2017-8547] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, and Windows Server 2012 and R2 allow an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8519."  
  
[CVE-2017-8548] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8549."  
  
[CVE-2017-8549] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system when Microsoft Edge improperly handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8499, CVE-2017-8520, CVE-2017-8521, and CVE-2017-8548."  
  
[CVE-2017-8552] "A kernel-mode driver in Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, and Windows 8 allows an elevation of privilege when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2017-0263."  
  
[CVE-2017-8553] "An information disclosure vulnerability exists in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows Server 2016 when the Windows kernel improperly handles objects in memory, aka ""GDI Information Disclosure Vulnerability""."  
  
[CVE-2017-8554] The kernel in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an authenticated attacker to obtain memory contents via a specially crafted application.  
  
[CVE-2017-8555] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8523 and CVE-2017-8530."  
  
[CVE-2017-8556] "Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8574."  
  
[CVE-2017-8558] "The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on 32-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703 does not properly scan a specially crafted file leading to memory corruption. aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability""."  
  
[CVE-2017-8561] "Windows kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka ""Windows Kernel Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8562] "Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows improperly handling calls to Advanced Local Procedure Call (ALPC), aka ""Windows ALPC Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8563] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Kerberos falling back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8564] "Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly initialize a memory address, aka ""Windows Kernel Information Disclosure Vulnerability""."  
  
[CVE-2017-8566] "Microsoft Windows 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows Input Method Editor (IME) improperly handling parameters in a method of a DCOM class, aka ""Windows IME Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8573] "Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8574 and CVE-2017-8556."  
  
[CVE-2017-8574] "Graphics in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8556."  
  
[CVE-2017-8575] "The kernel in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application, aka ""Microsoft Graphics Component Information Disclosure Vulnerability."""  
  
[CVE-2017-8576] "The graphics component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka ""Microsoft Graphics Component Elevation of Privilege Vulnerability."""  
  
[CVE-2017-8577] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8578] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8577, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8579] "The DirectX component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka ""DirectX Elevation of Privilege Vulnerability."""  
  
[CVE-2017-8580] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8577, CVE-2017-8578, CVE-2017-8581, and CVE-2017-8467."  
  
[CVE-2017-8581] "Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8577, and CVE-2017-8467."  
  
[CVE-2017-8582] "HTTP.sys in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when the component improperly handles objects in memory, aka ""Https.sys Information Disclosure Vulnerability""."  
  
[CVE-2017-8588] "Microsoft WordPad in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way it parses specially crafted files, aka ""WordPad Remote Code Execution Vulnerability""."  
  
[CVE-2017-8589] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way that Windows Search handles objects in memory, aka ""Windows Search Remote Code Execution Vulnerability""."  
  
[CVE-2017-8590] "Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way that the Windows Common Log File System (CLFS) driver handles objects in memory, aka ""Windows CLFS Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8592] "Microsoft browsers on when Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows RT 8.1, and Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a security feature bypass vulnerability when they improperly handle redirect requests, aka ""Microsoft Browser Security Feature Bypass""."  
  
[CVE-2017-8593] "Microsoft Win32k in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8594] "Internet Explorer on Microsoft Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability""."  
  
[CVE-2017-8595] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601,CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8596] "Microsoft Edge in Microsoft Windows 10 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8610, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8597] "Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8643 and CVE-2017-8648."  
  
[CVE-2017-8598] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8599] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8601] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8598 and CVE-2017-8609."  
  
[CVE-2017-8602] "Microsoft browsers on Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a spoofing vulnerability in the way they parse HTTP content, aka ""Microsoft Browser Spoofing Vulnerability."""  
  
[CVE-2017-8603] "Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8598, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8604] "Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8610, CVE-2017-8603, CVE-2017-8598, CVE-2017-8601, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8605] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8598, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8606] "Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609"  
  
[CVE-2017-8607] "Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8608, and CVE-2017-8609"  
  
[CVE-2017-8608] "Microsoft browsers in Microsoft Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8607, and CVE-2017-8609"  
  
[CVE-2017-8609] "Microsoft Internet Explorer in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Internet Explorer, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8610] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8595, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609."  
  
[CVE-2017-8611] "Microsoft Edge on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote attackers to spoof web content via a crafted web site, aka ""Microsoft Edge Spoofing Vulnerability."""  
  
[CVE-2017-8617] "Microsoft Edge in Windows 10 1703 Microsoft Edge allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Microsoft Edge Remote Code Execution Vulnerability."""  
  
[CVE-2017-8618] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 Internet Explorer in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability."" This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8619, CVE-2017-9598 and CVE-2017-8609."  
  
[CVE-2017-8619] "Microsoft Edge on Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability."" This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8618, CVE-2017-9598 and CVE-2017-8609."  
  
[CVE-2017-8628] "Microsoft Bluetooth Driver in Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 allows a spoofing vulnerability due to Microsoft's implementation of the Bluetooth stack, aka ""Microsoft Bluetooth Driver Spoofing Vulnerability""."  
  
[CVE-2017-8634] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8635] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that JavaScript engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8636] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8637] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to bypass Arbitrary Code Guard (ACG) due to how Microsoft Edge accesses memory in code compiled by the Edge Just-In-Time (JIT) compiler, aka ""Scripting Engine Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8638] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8639] "Microsoft Edge in Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8640] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8641] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8642] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to elevate privileges due to the way that Microsoft Edge validates JavaScript under specific conditions, aka ""Microsoft Edge Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8503."  
  
[CVE-2017-8643] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to leave a malicious website open during user clipboard activities, due to the way that Microsoft Edge handles clipboard events, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8648."  
  
[CVE-2017-8644] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8652 and CVE-2017-8662."  
  
[CVE-2017-8645] "Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8646] "Microsoft Edge in Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8647] "Microsoft Edge in Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8648] "Microsoft Edge in Microsoft Windows Version 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8597 and CVE-2017-8643."  
  
[CVE-2017-8649] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8650] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to exploit a security feature bypass due to Microsoft Edge not properly enforcing same-origin policies, aka ""Microsoft Edge Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8651] "Internet Explorer in Microsoft Windows Server 2008 SP2 and Windows Server 2012 allows an attacker to execute arbitrary code in the context of the current user due to Internet Explorer improperly accessing objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability""."  
  
[CVE-2017-8652] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to disclose information due to the way that Microsoft Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8662."  
  
[CVE-2017-8653] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to Microsoft browsers improperly accessing objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8669."  
  
[CVE-2017-8655] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8656] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8657] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8670, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8659] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system due to the Chakra scripting engine not properly handling objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability""."  
  
[CVE-2017-8660] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8661] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way affected Microsoft scripting engines render when handling objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability""."  
  
[CVE-2017-8662] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to disclose information due to how strings are validated in specific scenarios, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8644 and CVE-2017-8652."  
  
[CVE-2017-8666] "Microsoft Win32k in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly handle objects in memory, aka ""Win32k Information Disclosure Vulnerability""."  
  
[CVE-2017-8668] "The Volume Manager Extension Driver in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2 allows an attacker to run a specially crafted application and obtain kernel information, aka ""Volume Manager Extension Driver Information Disclosure Vulnerability""."  
  
[CVE-2017-8669] "Microsoft browsers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to Microsoft browsers improperly handling objects in memory while rendering content, aka ""Microsoft Browser Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8653."  
  
[CVE-2017-8670] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8671, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8671] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8672, and CVE-2017-8674."  
  
[CVE-2017-8672] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8674."  
  
[CVE-2017-8673] "The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 10 1703 allows an attacker to connect to a target system using RDP and send specially crafted requests, aka ""Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability."""  
  
[CVE-2017-8674] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8634, CVE-2017-8635, CVE-2017-8636, CVE-2017-8638, CVE-2017-8639, CVE-2017-8640, CVE-2017-8641, CVE-2017-8645, CVE-2017-8646, CVE-2017-8647, CVE-2017-8655, CVE-2017-8656, CVE-2017-8657, CVE-2017-8670, CVE-2017-8671, and CVE-2017-8672."  
  
[CVE-2017-8675] "The Windows Kernel-Mode Drivers component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when the Win32k component fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"".. This CVE ID is unique from CVE-2017-8720."  
  
[CVE-2017-8676] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8677] "The Windows GDI+ component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly discloses kernel memory addresses, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8678] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8677, CVE-2017-8680, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8679] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8709, and CVE-2017-8719."  
  
[CVE-2017-8680] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8677, CVE-2017-8681, and CVE-2017-8687."  
  
[CVE-2017-8681] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8677, and CVE-2017-8687."  
  
[CVE-2017-8682] "Windows graphics on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, Windows Server 2016, Microsoft Office Word Viewer, Microsoft Office 2007 Service Pack 3 , and Microsoft Office 2010 Service Pack 2 allows an attacker to execute remote code by the way it handles embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8683."  
  
[CVE-2017-8683] "Windows graphics on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows an attacker to execute remote code by the way it handles embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8682."  
  
[CVE-2017-8684] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1, allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8685 and CVE-2017-8688."  
  
[CVE-2017-8685] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8684 and CVE-2017-8688."  
  
[CVE-2017-8687] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Win32k Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8678, CVE-2017-8680, CVE-2017-8677, and CVE-2017-8681."  
  
[CVE-2017-8688] "Windows GDI+ on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows information disclosure by the way it discloses kernel memory addresses, aka ""Windows GDI+ Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8684 and CVE-2017-8685."  
  
[CVE-2017-8689] "The Microsoft Windows Kernel Mode Driver on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8694."  
  
[CVE-2017-8692] "The Windows Uniscribe component on Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote code execution vulnerability when it fails to properly handle objects in memory, aka ""Uniscribe Remote Code Execution Vulnerability""."  
  
[CVE-2017-8693] "The Microsoft Graphics Component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability in the way it handles objects in memory, aka ""Microsoft Graphics Information Disclosure Vulnerability""."  
  
[CVE-2017-8694] "The Microsoft Windows Kernel Mode Driver on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8689."  
  
[CVE-2017-8695] "Windows Uniscribe in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8696] "Windows Uniscribe in Microsoft Windows Server 2008 SP2 and R2 SP1  
[CVE-2017-8699] "Windows Shell in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to run arbitrary code in the context of the current user, due to the way that Windows Shell validates file copy destinations, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2017-8702] "Windows Error Reporting (WER) in Microsoft Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows an attacker to gain greater access to sensitive information and system functionality, due to the way that WER handles and executes files, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2017-8703] "The Microsoft Windows Subsystem for Linux on Microsoft Windows 10 1703 allows a denial of service vulnerability when it improperly handles objects in memory, aka ""Windows Subsystem for Linux Denial of Service Vulnerability""."  
  
[CVE-2017-8704] "The Windows Hyper-V component on Microsoft Windows 10 1607 and Windows Server 2016 allows a denial of service vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Denial of Service Vulnerability""."  
  
[CVE-2017-8706] "The Windows Hyper-V component on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8707] "The Windows Hyper-V component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8706, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8708] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8679, CVE-2017-8709, and CVE-2017-8719."  
  
[CVE-2017-8709] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8679, and CVE-2017-8719."  
  
[CVE-2017-8710] "The Microsoft Common Console Document (.msc) in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1 allows an attacker to read arbitrary files via an XML external entity (XXE) declaration, due to the way that the Microsoft Common Console Document (.msc) parses XML input containing a reference to an external entity, aka ""Windows Information Disclosure Vulnerability""."  
  
[CVE-2017-8711] "The Windows Hyper-V component on Microsoft Windows 10 1607 and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8706, CVE-2017-8712, and CVE-2017-8713."  
  
[CVE-2017-8712] "The Windows Hyper-V component on Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8706, and CVE-2017-8713."  
  
[CVE-2017-8713] "The Windows Hyper-V component on Microsoft Windows Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Hyper-V Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8707, CVE-2017-8711, CVE-2017-8712, and CVE-2017-8706."  
  
[CVE-2017-8714] "The Windows Hyper-V component on Microsoft Windows 8.1, Windows Server 2012 Gold and R2,, Windows 10 1607, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka ""Remote Desktop Virtual Host Remote Code Execution Vulnerability""."  
  
[CVE-2017-8715] "The Microsoft Device Guard on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a security feature bypass by the way it handles Windows PowerShell sessions, aka ""Windows Security Feature Bypass""."  
  
[CVE-2017-8716] "Windows Control Flow Guard in Microsoft Windows 10 Version 1703 allows an attacker to run a specially crafted application to bypass Control Flow Guard, due to the way that Control Flow Guard handles objects in memory, aka ""Windows Security Feature Bypass Vulnerability""."  
  
[CVE-2017-8717] "The Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to take control of an affected system, due to how it handles objects in memory, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8718."  
  
[CVE-2017-8718] "The Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to take control of an affected system, due to how it handles objects in memory, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8717."  
  
[CVE-2017-8719] "The Windows kernel component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it improperly handles objects in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2017-8708, CVE-2017-8709, and CVE-2017-8679."  
  
[CVE-2017-8720] "The Microsoft Windows graphics component on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when the Win32k component fails to properly handle objects in memory, aka ""Win32k Elevation of Privilege Vulnerability"". This CVE ID is unique from CVE-2017-8675."  
  
[CVE-2017-8723] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8754."  
  
[CVE-2017-8724] "Microsoft Edge in Microsoft Windows 10 Version 1703 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka ""Microsoft Edge Spoofing Vulnerability"". This CVE ID is unique from CVE-2017-8735."  
  
[CVE-2017-8726] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how affected Microsoft scripting engines handle objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-11794 and CVE-2017-11803."  
  
[CVE-2017-8727] "Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Windows Text Services Framework handles objects in memory, aka ""Windows Shell Memory Corruption Vulnerability""."  
  
[CVE-2017-8728] "Microsoft Windows PDF Library in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Windows PDF Library handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8737."  
  
[CVE-2017-8729] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8731] "Microsoft Edge in Microsoft Windows 10 1607 and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8734, CVE-2017-8751, and CVE-2017-11766."  
  
[CVE-2017-8733] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into believing that the user was visiting a legitimate website, due to the way that Internet Explorer handles specific HTML content, aka ""Internet Explorer Spoofing Vulnerability""."  
  
[CVE-2017-8734] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8751, and CVE-2017-11766."  
  
[CVE-2017-8735] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user by redirecting the user to a specially crafted website, due to the way that Microsoft Edge parses HTTP content, aka ""Microsoft Edge Spoofing Vulnerability"". This CVE ID is unique from CVE-2017-8724."  
  
[CVE-2017-8736] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to obtain specific information used in the parent domain, due to Microsoft browser parent domain verification in certain functionality, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2017-8737] "Microsoft Windows PDF Library in Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Windows PDF Library handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability"". This CVE ID is unique from CVE-2017-8728."  
  
[CVE-2017-8738] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8739] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to obtain information to further compromise the user's system, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability""."  
  
[CVE-2017-8740] "Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8741] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8747] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Internet Explorer accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8749."  
  
[CVE-2017-8748] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft browser JavaScript engines render content when handling objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8749] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Internet Explorer accesses objects in memory, aka ""Internet Explorer Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8747."  
  
[CVE-2017-8750] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user due to the way that Microsoft browsers access objects in memory, aka ""Microsoft Browser Memory Corruption Vulnerability""."  
  
[CVE-2017-8751] "Microsoft Edge in Microsoft Windows 1703 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Microsoft Edge Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8731, CVE-2017-8734, and CVE-2017-11766."  
  
[CVE-2017-8752] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8753, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8753] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the Microsoft Edge scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8755, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8754] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page containing malicious content, due to the way that the Edge Content Security Policy (CSP) validates certain specially crafted documents, aka ""Microsoft Edge Security Feature Bypass Vulnerability"". This CVE ID is unique from CVE-2017-8723."  
  
[CVE-2017-8755] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that the scripting engine handles objects in memory in Microsoft Edge, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8756, and CVE-2017-11764."  
  
[CVE-2017-8756] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way that Microsoft Edge accesses objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2017-8649, CVE-2017-8660, CVE-2017-8729, CVE-2017-8738, CVE-2017-8740, CVE-2017-8741, CVE-2017-8748, CVE-2017-8752, CVE-2017-8753, CVE-2017-8755, and CVE-2017-11764."  
  
[CVE-2017-8757] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to the way Microsoft Edge handles objects in memory, aka ""Microsoft Edge Remote Code Execution Vulnerability""."  
  
[CVE-2017-9511] The MultiPathResource class in Atlassian Fisheye and Crucible, before version 4.4.1 allows anonymous remote attackers to read arbitrary files via a path traversal vulnerability when Fisheye or Crucible is running on the Microsoft Windows operating system.  
  
[CVE-2018-0598] Untrusted search path vulnerability in Self-extracting archive files created by IExpress bundled with Microsoft Windows allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.  
  
[CVE-2018-0741] "The Color Management Module (Icm32.dll) in Windows 7 SP1 and Windows Server 2008 SP2 and R2 SP1 allows an information disclosure vulnerability due to the way objects are handled in memory, aka ""Microsoft Color Management Information Disclosure Vulnerability""."  
  
[CVE-2018-0749] "The Microsoft Server Message Block (SMB) Server in Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703 and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way SMB Server handles specially crafted files, aka ""Windows Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0755] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0760, CVE-2018-0761, and CVE-2018-0855."  
  
[CVE-2018-0758] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0760] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1, Windows Server 2008 R2, and Windows Server 2012 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0761, and CVE-2018-0855."  
  
[CVE-2018-0761] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0760, and CVE-2018-0855."  
  
[CVE-2018-0762] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0763] "Microsoft Edge in Microsoft Windows 10 1703 and 1709 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0839."  
  
[CVE-2018-0766] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the Microsoft Edge PDF Reader handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability""."  
  
[CVE-2018-0767] "Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0780 and CVE-2018-0800."  
  
[CVE-2018-0768] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0769] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0770] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0771] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows a security feature bypass, due to how Edge handles different-origin requests, aka ""Microsoft Edge Security Feature Bypass""."  
  
[CVE-2018-0772] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0773] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0774] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0775] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0776] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0777, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0777] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0778, and CVE-2018-0781."  
  
[CVE-2018-0778] "Microsoft Edge in Windows 10 1709 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0781."  
  
[CVE-2018-0780] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0800."  
  
[CVE-2018-0781] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, and CVE-2018-0778."  
  
[CVE-2018-0800] "Microsoft Edge in Microsoft Windows 10 1709 allows an attacker to obtain information to further compromise the user's system, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0767 and CVE-2018-0780."  
  
[CVE-2018-0803] "Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to access information from one domain and inject it into another domain, due to how Microsoft Edge enforces cross-domain policies, aka ""Microsoft Edge Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0811] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0813] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0814] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way objects are initialized in memory, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0815] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1 and Windows 7 SP1 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0816, and CVE-2018-0817."  
  
[CVE-2018-0816] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0815 and CVE-2018-0817."  
  
[CVE-2018-0817] "The Windows Graphics Device Interface (GDI) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to the way objects are handled in memory, aka ""Windows GDI Elevation of Privilege Vulnerability"". This CVE is unique from CVE-2018-0815 and CVE-2018-0816."  
  
[CVE-2018-0824] "A remote code execution vulnerability exists in ""Microsoft COM for Windows"" when it fails to properly handle serialized objects, aka ""Microsoft COM for Windows Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-0833] "The Microsoft Server Message Block 2.0 and 3.0 (SMBv2/SMBv3) client in Windows 8.1 and RT 8.1 and Windows Server 2012 R2 allows a denial of service vulnerability due to how specially crafted requests are handled, aka ""SMBv2/SMBv3 Null Dereference Denial of Service Vulnerability""."  
  
[CVE-2018-0834] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0835] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0836] "Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0837] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0838] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0839] "Microsoft Edge in Microsoft Windows 10 1703 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0763."  
  
[CVE-2018-0840] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0847] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2018-0855] "The Microsoft Windows Embedded OpenType (EOT) font engine in Microsoft Windows 7 SP1 and Windows Server 2008 R2 allows information disclosure, due to how the Windows EOT font engine handles embedded fonts, aka ""Windows EOT Font Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0755, CVE-2018-0760, and CVE-2018-0761."  
  
[CVE-2018-0856] "Microsoft Edge and ChakraCore in Microsoft Windows 10 1703 and 1709 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0857] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0859] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0860, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0860] "Microsoft Edge and ChakraCore in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0861, and CVE-2018-0866."  
  
[CVE-2018-0861] "Microsoft Edge in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, and CVE-2018-0866."  
  
[CVE-2018-0866] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0840, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, and CVE-2018-0861."  
  
[CVE-2018-0868] "Windows Installer in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege vulnerability due to how input is sanitized, aka ""Windows Installer Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0872] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0873] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0874] "ChakraCore and Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0876] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0889, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0878] "Windows Remote Assistance in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to how XML External Entities (XXE) are processed, aka ""Windows Remote Assistance Information Disclosure Vulnerability""."  
  
[CVE-2018-0879] "Microsoft Edge in Windows 10 1709 allows information disclosure, due to how Edge handles objects in memory, aka ""Microsoft Edge Information Disclosure Vulnerability""."  
  
[CVE-2018-0881] "The Microsoft Video Control in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an elevation of privilege due to how objects are handled in memory, aka ""Microsoft Video Control Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0883] "Windows Shell in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how file copy destinations are validated, aka ""Windows Shell Remote Code Execution Vulnerability""."  
  
[CVE-2018-0885] "The Microsoft Hyper-V Network Switch in 64-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows a denial of service vulnerability due to how input from a privileged user on a guest operating system is validated, aka ""Hyper-V Denial of Service Vulnerability""."  
  
[CVE-2018-0886] "The Credential Security Support Provider protocol (CredSSP) in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709 Windows Server 2016 and Windows Server, version 1709 allows a remote code execution vulnerability due to how CredSSP validates request during the authentication process, aka ""CredSSP Remote Code Execution Vulnerability""."  
  
[CVE-2018-0888] "The Microsoft Hyper-V Network Switch in 64-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to how guest operating system input is validated, aka ""Hyper-V Information Disclosure Vulnerability""."  
  
[CVE-2018-0889] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0893, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0891] "ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Internet Explorer and Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0939."  
  
[CVE-2018-0893] "Microsoft Edge in Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0889, CVE-2018-0925, and CVE-2018-0935."  
  
[CVE-2018-0894] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0895] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0896] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0897] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0898] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0899] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0900, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0900] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0901 and CVE-2018-0926."  
  
[CVE-2018-0901] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0926."  
  
[CVE-2018-0904] "The Windows kernel in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure vulnerability due to how memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability""."  
  
[CVE-2018-0926] "The Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 and RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and 1709, Windows Server 2016 and Windows Server, version 1709 allows an information disclosure vulnerability due to the way memory addresses are handled, aka ""Windows Kernel Information Disclosure Vulnerability"". This CVE is unique from CVE-2018-0811, CVE-2018-0813, CVE-2018-0814, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, and CVE-2018-0901."  
  
[CVE-2018-0927] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2018-0929] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow information disclosure, due to how Internet Explorer handles objects in memory, aka ""Internet Explorer Information Disclosure Vulnerability""."  
  
[CVE-2018-0930] "ChakraCore and Microsoft Edge in Microsoft Windows 10 1709 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0931] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0933, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0932] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, and Microsoft Edge and Internet Explorer in Windows 10 Gold, 1511, 1607, 1703, 1709, Windows Server 2016 and Windows Server, version 1709 allows information disclosure, due to how Microsoft browsers handle objects in memory, aka ""Microsoft Browser Information Disclosure Vulnerability""."  
  
[CVE-2018-0933] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0934, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0934] "ChakraCore and Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0936, and CVE-2018-0937."  
  
[CVE-2018-0935] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows remote code execution, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0876, CVE-2018-0889, CVE-2018-0893, and CVE-2018-0925."  
  
[CVE-2018-0936] "ChakraCore and Microsoft Windows 10 1709 allow remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, and CVE-2018-0937."  
  
[CVE-2018-0937] "ChakraCore and Microsoft Windows 10 1703 and 1709 allow remote code execution, due to how the Chakra scripting engine handles objects in memory, aka ""Chakra Scripting Engine Memory Corruption Vulnerability"". This CVE ID is unique from CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0930, CVE-2018-0931, CVE-2018-0933, CVE-2018-0934, and CVE-2018-0936."  
  
[CVE-2018-0939] "ChakraCore and Microsoft Edge in Windows 10 1703 and 1709 allow information disclosure, due to how the scripting engine handles objects in memory, aka ""Scripting Engine Information Disclosure Vulnerability"". This CVE ID is unique from CVE-2018-0891."  
  
[CVE-2018-0942] "Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow elevation of privilege, due to how Internet Explorer handles zone and integrity settings, aka ""Internet Explorer Elevation of Privilege Vulnerability""."  
  
[CVE-2018-0952] "An Elevation of Privilege vulnerability exists when Diagnostics Hub Standard Collector allows file creation in arbitrary locations, aka ""Diagnostic Hub Standard Collector Elevation Of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Microsoft Visual Studio, Windows 10 Servers."  
  
[CVE-2018-0986] "A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption, aka ""Microsoft Malware Protection Engine Remote Code Execution Vulnerability."" This affects Windows Defender, Windows Intune Endpoint Protection, Microsoft Security Essentials, Microsoft System Center Endpoint Protection, Microsoft Exchange Server, Microsoft System Center, Microsoft Forefront Endpoint Protection."  
  
[CVE-2018-1003] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10."  
  
[CVE-2018-1009] "An elevation of privilege vulnerability exists when Windows improperly handles objects in memory and incorrectly maps kernel memory, aka ""Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-1010] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1012, CVE-2018-1013, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1012] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1013, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1013] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1015, CVE-2018-1016."  
  
[CVE-2018-1015] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1016."  
  
[CVE-2018-1016] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1015."  
  
[CVE-2018-13399] The Microsoft Windows Installer for Atlassian Fisheye and Crucible before version 4.6.1 allows local attackers to escalate privileges because of weak permissions on the installation directory.  
  
[CVE-2018-15408] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15409] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15410] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15411] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15412] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15413] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15414] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15415] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15416] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15417] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15418] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15419] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15420] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15421] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15422] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15431] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or an email attachment and persuading the user to open the file by using the affected software. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2018-15437] A vulnerability in the system scanning component of Cisco Immunet and Cisco Advanced Malware Protection (AMP) for Endpoints running on Microsoft Windows could allow a local attacker to disable the scanning functionality of the product. This could allow executable files to be launched on the system without being analyzed for threats. The vulnerability is due to improper process resource handling. An attacker could exploit this vulnerability by gaining local access to a system running Microsoft Windows and protected by Cisco Immunet or Cisco AMP for Endpoints and executing a malicious file. A successful exploit could allow the attacker to prevent the scanning services from functioning properly and ultimately prevent the system from being protected from further intrusion.  
  
[CVE-2018-15490] An issue was discovered in ExpressVPN on Windows. The Xvpnd.exe process (which runs as a service with SYSTEM privileges) listens on TCP port 2015, which is used as an RPC interface for communication with the client side of the ExpressVPN application. A JSON-RPC protocol over HTTP is used for communication. The JSON-RPC XVPN.GetPreference and XVPN.SetPreference methods are vulnerable to path traversal, and allow reading and writing files on the file system on behalf of the service.  
  
[CVE-2018-16794] Microsoft ADFS 4.0 Windows Server 2016 and previous (Active Directory Federation Services) has an SSRF vulnerability via the txtBoxEmail parameter in /adfs/ls.  
  
[CVE-2018-3700] Code injection vulnerability in the installer for Intel(R) USB 3.0 eXtensible Host Controller Driver for Microsoft Windows 7 before version 5.0.4.43v2 may allow a user to potentially enable escalation of privilege via local access.  
  
[CVE-2018-4858] A vulnerability has been identified in IEC 61850 system configurator (All versions < V5.80), DIGSI 5 (affected as IEC 61850 system configurator is incorporated) (All versions < V7.80), DIGSI 4 (All versions < V4.93), SICAM PAS/PQS (All versions < V8.11), SICAM PQ Analyzer (All versions < V3.11), SICAM SCC (All versions < V9.02 HF3). A service of the affected products listening on all of the host's network interfaces on either port 4884/TCP, 5885/TCP, or port 5886/TCP could allow an attacker to either exfiltrate limited data from the system or to execute code with Microsoft Windows user permissions. Successful exploitation requires an attacker to be able to send a specially crafted network request to the vulnerable service and a user interacting with the service's client application on the host. In order to execute arbitrary code with Microsoft Windows user permissions, an attacker must be able to plant the code in advance on the host by other means. The vulnerability has limited impact to confidentiality and integrity of the affected system. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.  
  
[CVE-2018-5440] A Stack-based Buffer Overflow issue was discovered in 3S-Smart CODESYS Web Server. Specifically: all Microsoft Windows (also WinCE) based CODESYS web servers running stand-alone Version 2.3, or as part of the CODESYS runtime system running prior to Version V1.1.9.19. A crafted request may cause a buffer overflow and could therefore execute arbitrary code on the web server or lead to a denial-of-service condition due to a crash in the web server.  
  
[CVE-2018-6661] DLL Side-Loading vulnerability in Microsoft Windows Client in McAfee True Key before 4.20.110 allows local users to gain privilege elevation via not verifying a particular DLL file signature.  
  
[CVE-2018-6664] Application Protections Bypass vulnerability in Microsoft Windows in McAfee Data Loss Prevention (DLP) Endpoint before 10.0.500 and DLP Endpoint before 11.0.400 allows authenticated users to bypass the product block action via a command-line utility.  
  
[CVE-2018-6674] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 13 allows local users to spawn unrelated processes with elevated privileges via the system administrator granting McTray.exe elevated privileges (by default it runs with the current user's privileges).  
  
[CVE-2018-6687] Loop with Unreachable Exit Condition ('Infinite Loop') in McAfee GetSusp (GetSusp) 3.0.0.461 and earlier allows attackers to DoS a manual GetSusp scan via while scanning a specifically crafted file . GetSusp is a free standalone McAfee tool that runs on several versions of Microsoft Windows.  
  
[CVE-2018-6690] Accessing, modifying, or executing executable files vulnerability in Microsoft Windows client in McAfee Application and Change Control (MACC) 8.0.0 Hotfix 4 and earlier allows authenticated users to execute arbitrary code via file transfer from external system.  
  
[CVE-2018-6700] DLL Search Order Hijacking vulnerability in Microsoft Windows Client in McAfee True Key (TK) before 5.1.165 allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6755] Weak Directory Permission Vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6756] Authentication Abuse vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute unauthorized commands via specially crafted malware.  
  
[CVE-2018-6757] Privilege Escalation vulnerability in Microsoft Windows client in McAfee True Key (TK) 5.1.230.7 and earlier allows local users to execute arbitrary code via specially crafted malware.  
  
[CVE-2018-6765] Swisscom MySwisscomAssistant 2.17.1.1065 contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system. This vulnerability exists due to the way .dll files are loaded. It allows an attacker to load a .dll of the attacker's choosing that could execute arbitrary code without the user's knowledge. The specific flaw exists within the handling of several DLLs (dwmapi.dll, IPHLPAPI.DLL, WindowsCodecs.dll, RpcRtRemote.dll, CRYPTSP.dll, rasadhlp.dll, DNSAPI.dll, ntmarta.dll, netbios.dll, olepro32.dll, security.dll, winhttp.dll, WINSTA.dll) loaded by the MySwisscomAssistant\_Setup.exe process.  
  
[CVE-2018-7249] An issue was discovered in secdrv.sys as shipped in Microsoft Windows Vista, Windows 7, Windows 8, and Windows 8.1 before KB3086255, and as shipped in Macrovision SafeDisc. Two carefully timed calls to IOCTL 0xCA002813 can cause a race condition that leads to a use-after-free. When exploited, an unprivileged attacker can run arbitrary code in the kernel.  
  
[CVE-2018-7250] An issue was discovered in secdrv.sys as shipped in Microsoft Windows Vista, Windows 7, Windows 8, and Windows 8.1 before KB3086255, and as shipped in Macrovision SafeDisc. An uninitialized kernel pool allocation in IOCTL 0xCA002813 allows a local unprivileged attacker to leak 16 bits of uninitialized kernel PagedPool data.  
  
[CVE-2018-8116] "A denial of service vulnerability exists in the way that Windows handles objects in memory, aka ""Microsoft Graphics Component Denial of Service Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8218] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers."  
  
[CVE-2018-8253] "An elevation of privilege vulnerability exists when Microsoft Cortana allows arbitrary website browsing on the lockscreen, aka ""Microsoft Cortana Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10."  
  
[CVE-2018-8256] "A remote code execution vulnerability exists when PowerShell improperly handles specially crafted files, aka ""Microsoft PowerShell Remote Code Execution Vulnerability."" This affects Windows RT 8.1, PowerShell Core 6.0, Microsoft.PowerShell.Archive 1.2.2.0, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, Windows Server 2019, Windows 7, Windows Server 2012 R2, PowerShell Core 6.1, Windows 10 Servers, Windows 10, Windows 8.1."  
  
[CVE-2018-8307] "A security feature bypass vulnerability exists when Microsoft WordPad improperly handles embedded OLE objects, aka ""WordPad Security Feature Bypass Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8332] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Win32k Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Microsoft Office, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8333] "An Elevation of Privilege vulnerability exists in Filter Manager when it improperly handles objects in memory, aka ""Microsoft Filter Manager Elevation Of Privilege Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8335] "A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server, aka ""Windows SMB Denial of Service Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8344] "A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka ""Microsoft Graphics Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8345] "A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka ""LNK Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8346."  
  
[CVE-2018-8346] "A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka ""LNK Remote Code Execution Vulnerability."" This affects Windows Server 2008, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8345."  
  
[CVE-2018-8347] "An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka ""Windows Kernel Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8349] "A remote code execution vulnerability exists in ""Microsoft COM for Windows"" when it fails to properly handle serialized objects, aka ""Microsoft COM for Windows Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8350] "A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory, aka ""Windows PDF Remote Code Execution Vulnerability."" This affects Windows 10 Servers, Windows 10."  
  
[CVE-2018-8392] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8393."  
  
[CVE-2018-8393] "A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8392."  
  
[CVE-2018-8407] "An information disclosure vulnerability exists when ""Kernel Remote Procedure Call Provider"" driver improperly initializes objects in memory, aka ""MSRPC Information Disclosure Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8415] "A tampering vulnerability exists in PowerShell that could allow an attacker to execute unlogged code, aka ""Microsoft PowerShell Tampering Vulnerability."" This affects Windows 7, PowerShell Core 6.1, Windows Server 2012 R2, Windows RT 8.1, PowerShell Core 6.0, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8417] "A security feature bypass vulnerability exists in Microsoft JScript that could allow an attacker to bypass Device Guard, aka ""Microsoft JScript Security Feature Bypass Vulnerability."" This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers."  
  
[CVE-2018-8420] "A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka ""MS XML Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8423] "A remote code execution vulnerability exists in the Microsoft JET Database Engine, aka ""Microsoft JET Database Engine Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8427] "An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Information Disclosure Vulnerability."" This affects Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Windows Server 2008, Microsoft PowerPoint Viewer, Microsoft Excel Viewer."  
  
[CVE-2018-8432] "A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Remote Code Execution Vulnerability."" This affects Windows 7, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft Excel Viewer, Microsoft PowerPoint Viewer, Windows Server 2019, Windows Server 2008 R2, Windows 10, Windows Server 2008."  
  
[CVE-2018-8433] "An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka ""Microsoft Graphics Component Information Disclosure Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8436] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8437, CVE-2018-8438."  
  
[CVE-2018-8437] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8436, CVE-2018-8438."  
  
[CVE-2018-8438] "A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka ""Windows Hyper-V Denial of Service Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8436, CVE-2018-8437."  
  
[CVE-2018-8444] "An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka ""Windows SMB Information Disclosure Vulnerability."" This affects Windows Server 2012, Windows 10, Windows 8.1, Windows RT 8.1, Windows Server 2012 R2."  
  
[CVE-2018-8471] "An elevation of privilege vulnerability exists in the way that the Microsoft RemoteFX Virtual GPU miniport driver handles objects in memory, aka ""Microsoft RemoteFX Virtual GPU miniport driver Elevation of Privilege Vulnerability."" This affects Windows Server 2016, Windows 10, Windows 8.1, Windows 7, Windows Server 2019."  
  
[CVE-2018-8494] "A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka ""MS XML Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8506] "An Information Disclosure vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka ""Microsoft Windows Codecs Library Information Disclosure Vulnerability."" This affects Windows 10 Servers, Windows 10, Windows Server 2019."  
  
[CVE-2018-8547] "A cross-site-scripting (XSS) vulnerability exists when an open source customization for Microsoft Active Directory Federation Services (AD FS) does not properly sanitize a specially crafted web request to an affected AD FS server, aka ""Active Directory Federation Services XSS Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8553] "A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka ""Microsoft Graphics Components Remote Code Execution Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10."  
  
[CVE-2018-8599] "An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka ""Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability."" This affects Microsoft Visual Studio, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers."  
  
[CVE-2018-8634] "A remote code execution vulnerability exists in Windows where Microsoft text-to-speech fails to properly handle objects in the memory, aka ""Microsoft Text-To-Speech Remote Code Execution Vulnerability."" This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers."  
  
[CVE-2018-8853] Philips Brilliance CT devices operate user functions from within a contained kiosk in a Microsoft Windows operating system. Windows boots by default with elevated Windows privileges, enabling a kiosk application, user, or an attacker to potentially attain unauthorized elevated privileges in Brilliance 64 version 2.6.2 and prior, Brilliance iCT versions 4.1.6 and prior, Brillance iCT SP versions 3.2.4 and prior, and Brilliance CT Big Bore 2.3.5 and prior. Also, attackers may gain access to unauthorized resources from the underlying Windows operating system.  
  
[CVE-2019-0232] When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).  
  
[CVE-2019-0543] "An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka ""Microsoft Windows Elevation of Privilege Vulnerability."" This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers."  
  
[CVE-2019-0555] "An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka ""Microsoft XmlDocument Elevation of Privilege Vulnerability."" This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers."  
  
[CVE-2019-0630] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.  
  
[CVE-2019-0633] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630.  
  
[CVE-2019-0690] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701.  
  
[CVE-2019-0695] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0701.  
  
[CVE-2019-0701] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0695.  
  
[CVE-2019-0710] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713.  
  
[CVE-2019-0711] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713.  
  
[CVE-2019-0712] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399.  
  
[CVE-2019-0713] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711.  
  
[CVE-2019-0714] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0715, CVE-2019-0717, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0715] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0717, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0717] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0718, CVE-2019-0723.  
  
[CVE-2019-0718] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0717, CVE-2019-0723.  
  
[CVE-2019-0723] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0714, CVE-2019-0715, CVE-2019-0717, CVE-2019-0718.  
  
[CVE-2019-0734] An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936.  
  
[CVE-2019-0766] An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2019-0885] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2019-0928] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2019-0936] An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734.  
  
[CVE-2019-0966] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2019-1019] A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1040] A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.  
  
[CVE-2019-1074] An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic link attack. An attacker who successfully exploited this vulnerability could potentially access unauthorized information. The update addresses this vulnerability by not allowing symbolic links in these scenarios., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1082.  
  
[CVE-2019-1078] An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1148, CVE-2019-1153.  
  
[CVE-2019-1082] An elevation of privilege vulnerability exists in Microsoft Windows where a certain DLL, with Local Service privilege, is vulnerable to race planting a customized DLL.An attacker who successfully exploited this vulnerability could potentially elevate privilege to SYSTEM.The update addresses this vulnerability by requiring SYSTEM privileges for a certain DLL., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1074.  
  
[CVE-2019-1089] An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this vulnerability, a low level authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how rpcss.dll handles these requests., aka 'Windows RPCSS Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1144] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1145] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1148] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1078, CVE-2019-1153.  
  
[CVE-2019-1149] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1150, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1150] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1151, CVE-2019-1152.  
  
[CVE-2019-1151] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1152.  
  
[CVE-2019-1152] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1144, CVE-2019-1145, CVE-2019-1149, CVE-2019-1150, CVE-2019-1151.  
  
[CVE-2019-1153] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1078, CVE-2019-1148.  
  
[CVE-2019-1166] A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.  
  
[CVE-2019-1168] An elevation of privilege exists in the p2pimsvc service where an attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges.To exploit this vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability'.  
  
[CVE-2019-11684] "Improper Access Control in the RCP+ server of the Bosch Video Recording Manager (VRM) component allows arbitrary and unauthenticated access to a limited subset of certificates, stored in the underlying Microsoft Windows operating system. The fixed versions implement modified authentication checks. Prior releases of VRM software version 3.70 are considered unaffected. This vulnerability affects VRM v3.70.x, v3.71 < v3.71.0034 and v3.81 < 3.81.0050  
[CVE-2019-1172] An information disclosure vulnerability exists in Azure Active Directory (AAD) Microsoft Account (MSA) during the login request session, aka 'Windows Information Disclosure Vulnerability'.  
  
[CVE-2019-1177] An elevation of privilege vulnerability exists in the way that the rpcss.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1173, CVE-2019-1174, CVE-2019-1175, CVE-2019-1178, CVE-2019-1179, CVE-2019-1180, CVE-2019-1184, CVE-2019-1186.  
  
[CVE-2019-1188] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2019-1198] An elevation of privilege exists in SyncController.dll, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1270] An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Microsoft Windows Store Installer Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1280] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2019-1309] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1310, CVE-2019-1399.  
  
[CVE-2019-1310] A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1399.  
  
[CVE-2019-1316] An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1317] A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.  
  
[CVE-2019-1318] A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.  
  
[CVE-2019-1320] An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.  
  
[CVE-2019-1321] An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL), aka 'Microsoft Windows CloudStore Elevation of Privilege Vulnerability'.  
  
[CVE-2019-1322] An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.  
  
[CVE-2019-1323] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.  
  
[CVE-2019-1336] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.  
  
[CVE-2019-1338] A security feature bypass vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLMv2 protection if a client is also sending LMv2 responses, aka 'Windows NTLM Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1340] An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1322.  
  
[CVE-2019-1381] An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'.  
  
[CVE-2019-1384] A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2019-1399] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310.  
  
[CVE-2019-1409] An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'.  
  
[CVE-2019-1419] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456.  
  
[CVE-2019-1430] A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'Microsoft Windows Media Foundation Remote Code Execution Vulnerability'.  
  
[CVE-2019-1456] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419.  
  
[CVE-2019-1484] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2019-15162] rpcapd/daemon.c in libpcap before 1.9.1 on non-Windows platforms provides details about why authentication failed, which might make it easier for attackers to enumerate valid usernames.  
  
[CVE-2019-15283] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15284] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15285] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15286] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-15287] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1637] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1638] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1639] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1640] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1641] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1771] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1772] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-1773] A vulnerability in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file via a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system.  
  
[CVE-2019-18232] SafeNet Sentinel LDK License Manager, all versions prior to 7.101(only Microsoft Windows versions are affected) is vulnerable when configured as a service. This vulnerability may allow an attacker with local access to create, write, and/or delete files in system folder using symbolic links, leading to a privilege escalation. This vulnerability could also be used by an attacker to execute a malicious DLL, which could impact the integrity and availability of the system.  
  
[CVE-2019-18631] The Windows component of Centrify Authentication and Privilege Elevation Services 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.5.0, 3.5.1 (18.8), 3.5.2 (18.11), and 3.6.0 (19.6) does not properly handle an unspecified exception during use of partially trusted assemblies to serialize input data, which allows attackers to execute arbitrary code inside the Centrify process via (1) a crafted application that makes a pipe connection to the process and sends malicious serialized data or (2) a crafted Microsoft Management Console snap-in control file.  
  
[CVE-2019-18913] "A potential security vulnerability with pre-boot DMA may allow unauthorized UEFI code execution using open-case attacks. This industry-wide issue requires physically accessing internal expansion slots with specialized hardware and software tools to modify UEFI code in memory. This affects HP Intel-based Business PCs that support Microsoft Windows 10 Kernel DMA protection. Affected versions depend on platform (prior to 01.04.02  
[CVE-2019-1924] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1925] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1926] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1927] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1928] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-1929] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2019-19363] An issue was discovered in Ricoh (including Savin and Lanier) Windows printer drivers prior to 2020 that allows attackers local privilege escalation. Affected drivers and versions are: PCL6 Driver for Universal Print - Version 4.0 or later PS Driver for Universal Print - Version 4.0 or later PC FAX Generic Driver - All versions Generic PCL5 Driver - All versions RPCS Driver - All versions PostScript3 Driver - All versions PCL6 (PCL XL) Driver - All versions RPCS Raster Driver - All version  
  
[CVE-2019-20406] The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.  
  
[CVE-2019-2390] "An unprivileged user or program on Microsoft Windows which can create OpenSSL configuration files in a fixed location may cause utility programs shipped with MongoDB server to run attacker defined code as the user running the utility. This issue affects: MongoDB Inc. MongoDB Server 4.0 prior to 4.0.11  
[CVE-2019-3582] Privilege Escalation vulnerability in Microsoft Windows client in McAfee Endpoint Security (ENS) 10.6.1 and earlier allows local users to gain elevated privileges via a specific set of circumstances.  
  
[CVE-2019-3585] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow local users to interact with the On-Access Scan Messages - Threat Alert Window with elevated privileges via running McAfee Tray with elevated privileges.  
  
[CVE-2019-3587] DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.18 allows local users to execute arbitrary code via execution from a compromised folder.  
  
[CVE-2019-3588] Privilege Escalation vulnerability in Microsoft Windows client (McTray.exe) in McAfee VirusScan Enterprise (VSE) 8.8 prior to Patch 14 may allow unauthorized users to interact with the On-Access Scan Messages - Threat Alert Window when the Windows Login Screen is locked.  
  
[CVE-2019-3593] Exploitation of Privilege/Trust vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Prior to 16.0.R18 allows local users to bypass product self-protection, tamper with policies and product files, and uninstall McAfee software without permission via specially crafted malware.  
  
[CVE-2019-3610] Data Leakage Attacks vulnerability in Microsoft Windows client in McAfee True Key (TK) 3.1.9211.0 and earlier allows local users to expose confidential data via specially crafted malware.  
  
[CVE-2019-3646] DLL Search Order Hijacking vulnerability in Microsoft Windows client in McAfee Total Protection (MTP) Free Antivirus Trial 16.0.R18 and earlier allows local users to execute arbitrary code via execution from a compromised folder placed by an attacker with administrator rights.  
  
[CVE-2019-3648] A Privilege Escalation vulnerability in the Microsoft Windows client in McAfee Total Protection 16.0.R22 and earlier allows administrators to execute arbitrary code via carefully placing malicious files in specific locations protected by administrator permission.  
  
[CVE-2019-3654] Authentication Bypass vulnerability in the Microsoft Windows client in McAfee Client Proxy (MCP) prior to 3.0.0 allows local user to bypass scanning of web traffic and gain access to blocked sites for a short period of time via generating an authorization key on the client which should only be generated by the network administrator.  
  
[CVE-2019-3667] DLL Search Order Hijacking vulnerability in the Microsoft Windows client in McAfee Tech Check 3.0.0.17 and earlier allows local users to execute arbitrary code via the local folder placed there by an attacker.  
  
[CVE-2019-3880] A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.  
  
[CVE-2019-4732] IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.  
  
[CVE-2019-6265] The Scripting and AutoUpdate functionality in Cordaware bestinformed Microsoft Windows client versions before 6.2.1.0 are affected by insecure implementations which allow remote attackers to execute arbitrary commands and escalate privileges.  
  
[CVE-2019-6266] Cordaware bestinformed Microsoft Windows client before 6.2.1.0 is affected by insecure SSL certificate verification and insecure access patterns. These issues allow remote attackers to downgrade encrypted connections to cleartext.  
  
[CVE-2019-9510] A vulnerability in Microsoft Windows 10 1803 and Windows Server 2019 and later systems can allow authenticated RDP-connected clients to gain access to user sessions without needing to interact with the Windows lock screen. Should a network anomaly trigger a temporary RDP disconnect, Automatic Reconnection of the RDP session will be restored to an unlocked state, regardless of how the remote system was left. By interrupting network connectivity of a system, an attacker with access to a system being used as a Windows RDP client can gain access to a connected remote system, regardless of whether or not the remote system was locked. This issue affects Microsoft Windows 10, version 1803 and later, and Microsoft Windows Server 2019, version 2019 and later.  
  
[CVE-2020-0616] A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.  
  
[CVE-2020-0622] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-0635] An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0644.  
  
[CVE-2020-0641] An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-0644] An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0635.  
  
[CVE-2020-0661] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751.  
  
[CVE-2020-0684] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-0687] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.  
  
[CVE-2020-0729] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-0751] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0661.  
  
[CVE-2020-0796] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.  
  
[CVE-2020-0799] An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka 'Windows Kernel Elevation of Privilege Vulnerability'.  
  
[CVE-2020-0890] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0904.  
  
[CVE-2020-0904] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0890.  
  
[CVE-2020-0921] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1083.  
  
[CVE-2020-0922] A remote code execution vulnerability exists in the way that Microsoft COM for Windows handles objects in memory, aka 'Microsoft COM for Windows Remote Code Execution Vulnerability'.  
  
[CVE-2020-0938] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.  
  
[CVE-2020-0965] A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'.  
  
[CVE-2020-0982] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0987, CVE-2020-1005.  
  
[CVE-2020-0987] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-1005.  
  
[CVE-2020-1005] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0982, CVE-2020-0987.  
  
[CVE-2020-1009] An elevation of privilege vulnerability exists in the way that the Microsoft Store Install Service handles file operations in protected locations, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0934, CVE-2020-0983, CVE-2020-1011, CVE-2020-1015.  
  
[CVE-2020-1010] An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079.  
  
[CVE-2020-1013] An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates, aka 'Group Policy Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1014] An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1018] An information disclosure vulnerability exists when Microsoft Dynamics Business Central/NAV on-premise does not properly hide the value of a masked field when showing the records as a chart page.The attacker who successfully exploited the vulnerability could see the information that are in a masked field.The security update addresses the vulnerability by updating the rendering engine the Windows client to properly detect masked fields and render the content as masked., aka 'Microsoft Dynamics Business Central/NAV Information Disclosure'.  
  
[CVE-2020-1020] A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0938.  
  
[CVE-2020-1068] An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1079.  
  
[CVE-2020-1079] An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068.  
  
[CVE-2020-1083] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0921.  
  
[CVE-2020-1118] A denial of service vulnerability exists in the Windows implementation of Transport Layer Security (TLS) when it improperly handles certain key exchanges, aka 'Microsoft Windows Transport Layer Security Denial of Service Vulnerability'.  
  
[CVE-2020-1129] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1319.  
  
[CVE-2020-1160] An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-1163] An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1170.  
  
[CVE-2020-1170] An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163.  
  
[CVE-2020-1206] An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.  
  
[CVE-2020-1243] A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'.  
  
[CVE-2020-1281] A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.  
  
[CVE-2020-1284] A denial of service vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Denial of Service Vulnerability'.  
  
[CVE-2020-1299] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-1300] A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.The update addresses the vulnerability by correcting how Windows handles cabinet files., aka 'Windows Remote Code Execution Vulnerability'.  
  
[CVE-2020-1301] A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'.  
  
[CVE-2020-13162] A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5.3 R70 for Windows (which runs as NT AUTHORITY/SYSTEM) allows unprivileged users to run a Microsoft Installer executable with elevated privileges.  
  
[CVE-2020-1319] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1129.  
  
[CVE-2020-1351] An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'.  
  
[CVE-2020-1383] An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'.  
  
[CVE-2020-1408] A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.  
  
[CVE-2020-1421] A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.  
  
[CVE-2020-1425] A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1457.  
  
[CVE-2020-1457] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1425.  
  
[CVE-2020-1471] An elevation of privilege vulnerability exists when Microsoft Windows CloudExperienceHost fails to check COM objects, aka 'Windows CloudExperienceHost Elevation of Privilege Vulnerability'.  
  
[CVE-2020-1507] An elevation of privilege vulnerability exists in the way that Microsoft COM for Windows handles objects in memory, aka 'Microsoft COM for Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-15145] In Composer-Setup for Windows before version 6.0.0, if the developer's computer is shared with other users, a local attacker may be able to exploit the following scenarios. 1. A local regular user may modify the existing `C:\ProgramData\ComposerSetup\bin\composer.bat` in order to get elevated command execution when composer is run by an administrator. 2. A local regular user may create a specially crafted dll in the `C:\ProgramData\ComposerSetup\bin` folder in order to get Local System privileges. See: https://itm4n.github.io/windows-server-netman-dll-hijacking. 3. If the directory of the php.exe selected by the user is not in the system path, it is added without checking that it is admin secured, as per Microsoft guidelines. See: https://msrc-blog.microsoft.com/2018/04/04/triaging-a-dll-planting-vulnerability.  
  
[CVE-2020-1560] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1574, CVE-2020-1585.  
  
[CVE-2020-1574] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1585.  
  
[CVE-2020-1585] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1574.  
  
[CVE-2020-16877] An elevation of privilege vulnerability exists when Microsoft Windows improperly handles reparse points, aka 'Windows Elevation of Privilege Vulnerability'.  
  
[CVE-2020-16910] A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location.To exploit this vulnerability, an attacker could run a specially crafted application to bypass Unified Extensible Firmware Interface (UEFI) variable security in Windows.The security update addresses the vulnerability by correcting security feature behavior to enforce permissions., aka 'Windows Security Feature Bypass Vulnerability'.  
  
[CVE-2020-17022] A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'.  
  
[CVE-2020-17162] Microsoft Windows Security Feature Bypass Vulnerability  
  
[CVE-2020-24556] A vulnerability in Trend Micro Apex One, OfficeScan XG SP1, Worry-Free Business Security 10 SP1 and Worry-Free Business Security Services on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.  
  
[CVE-2020-24557] A vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 on Microsoft Windows may allow an attacker to manipulate a particular product folder to disable the security temporarily, abuse a specific Windows function and attain privilege escalation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note that version 1909 (OS Build 18363.719) of Microsoft Windows 10 mitigates hard links, but previous versions are affected.  
  
[CVE-2020-24562] A vulnerability in Trend Micro OfficeScan XG SP1 on Microsoft Windows may allow an attacker to create a hard link to any file on the system, which then could be manipulated to gain a privilege escalation and code execution. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This CVE is similar, but not identical to CVE-2020-24556.  
  
[CVE-2020-25182] Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x searches for and loads DLLs as dynamic libraries. Uncontrolled loading of dynamic libraries could allow a local, unauthenticated attacker to execute arbitrary code. This vulnerability only affects ISaGRAF Runtime when running on Microsoft Windows systems.  
  
[CVE-2020-3127] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3128] Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements within a Webex recording that is stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a malicious ARF or WRF file to a user through a link or email attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3194] A vulnerability in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.  
  
[CVE-2020-3319] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.  
  
[CVE-2020-3321] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.  
  
[CVE-2020-3322] A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.  
  
[CVE-2020-36233] The Microsoft Windows Installer for Atlassian Bitbucket Server and Data Center before version 6.10.9, 7.x before 7.6.4, and from version 7.7.0 before 7.10.1 allows local attackers to escalate privileges because of weak permissions on the installation directory.  
  
[CVE-2020-36603] The HoYoVerse (formerly miHoYo) Genshin Impact mhyprot2.sys 1.0.0.0 anti-cheat driver does not adequately restrict unprivileged function calls, allowing local, unprivileged users to execute arbitrary code with SYSTEM privileges on Microsoft Windows systems. The mhyprot2.sys driver must first be installed by a user with administrative privileges.  
  
[CVE-2020-4739] IBM DB2 Accessories Suite for Linux, UNIX, and Windows, DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 188149.  
  
[CVE-2020-4767] IBM Sterling Connect Direct for Microsoft Windows 4.7, 4.8, 6.0, and 6.1 could allow a remote attacker to cause a denial of service, caused by a buffer over-read. Bysending a specially crafted request, the attacker could cause the application to crash. IBM X-Force ID: 188906.  
  
[CVE-2020-5384] Authentication Bypass Vulnerability RSA MFA Agent 2.0 for Microsoft Windows contains an Authentication Bypass vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability by using an alternate path to bypass authentication in order to gain full access to the system.  
  
[CVE-2020-7205] "A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. \*\*Note:\*\* This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. \*\*Note:\*\* This DBX update mitigates the GRUB2 issue with insmod enabled, and the ""Boot Hole"" issue for HPE signed GRUB2 applications."  
  
[CVE-2020-7299] "Cleartext Storage of Sensitive Information in Memory vulnerability in Microsoft Windows client in McAfee True Key (TK) prior to 6.2.109.2 allows a local user logged in with administrative privileges to access to another user&#8217  
[CVE-2020-7320] Protection Mechanism Failure vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2020 Update allows local administrator to temporarily reduce the detection capability allowing otherwise detected malware to run via stopping certain Microsoft services.  
  
[CVE-2020-7335] Privilege Escalation vulnerability in Microsoft Windows client McAfee Total Protection (MTP) prior to 16.0.29 allows local users to gain elevated privileges via careful manipulation of a folder by creating a junction link. This exploits a lack of protection through a timing issue and is only exploitable in a small time window.  
  
[CVE-2021-1372] A vulnerability in Cisco Webex Meetings Desktop App and Webex Productivity Tools for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. This vulnerability is due to the unsafe usage of shared memory by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens. Note: To exploit this vulnerability, an attacker must have valid credentials on a Microsoft Windows end-user system and must log in after another user has already authenticated with Webex on the same end-user system.  
  
[CVE-2021-1710] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-21513] Dell EMC OpenManage Server Administrator (OMSA) version 9.5 Microsoft Windows installations with Distributed Web Server (DWS) enabled configuration contains an authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain admin access on the affected system.  
  
[CVE-2021-21706] In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.  
  
[CVE-2021-24076] Microsoft Windows VMSwitch Information Disclosure Vulnerability  
  
[CVE-2021-24081] Microsoft Windows Codecs Library Remote Code Execution Vulnerability  
  
[CVE-2021-26432] Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability  
  
[CVE-2021-26433] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-36926, CVE-2021-36932, CVE-2021-36933.  
  
[CVE-2021-26881] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-26887] Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability  
  
[CVE-2021-28317] Microsoft Windows Codecs Library Information Disclosure Vulnerability  
  
[CVE-2021-31184] Microsoft Windows Infrared Data Association (IrDA) Information Disclosure Vulnerability  
  
[CVE-2021-32022] A low privileged delete vulnerability using CEF RPC server of BlackBerry Protect for Windows version(s) versions 1574 and earlier could allow an attacker to potentially execute code in the context of a BlackBerry Cylance service that has admin rights on the system and gaining the ability to delete data from the local system.  
  
[CVE-2021-34439] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34441, CVE-2021-34503.  
  
[CVE-2021-34441] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34503.  
  
[CVE-2021-34471] Microsoft Windows Defender Elevation of Privilege Vulnerability  
  
[CVE-2021-34503] Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34441.  
  
[CVE-2021-34579] "In Phoenix Contact: FL MGUARD DM version 1.12.0 and 1.13.0 access to the Apache web server being installed as part of the FL MGUARD DM on Microsoft Windows does not require login credentials even if configured during installation.Attackers with network access to the Apache web server can download and therefore read mGuard configuration profiles (&#8220  
[CVE-2021-35211] Microsoft discovered a remote code execution (RCE) vulnerability in the SolarWinds Serv-U product utilizing a Remote Memory Escape Vulnerability. If exploited, a threat actor may be able to gain privileged access to the machine hosting Serv-U Only. SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows before 15.2.3 HF2 are affected by this vulnerability.  
  
[CVE-2021-36745] A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass authentication on affected installations.  
  
[CVE-2021-36926] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36932, CVE-2021-36933.  
  
[CVE-2021-36932] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36926, CVE-2021-36933.  
  
[CVE-2021-36933] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-26433, CVE-2021-36926, CVE-2021-36932.  
  
[CVE-2021-38505] "Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats  
[CVE-2021-38634] Microsoft Windows Update Client Elevation of Privilege Vulnerability  
  
[CVE-2021-39032] IBM Sterling Gentran:Server for Microsoft Windows 5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 213962.  
  
[CVE-2021-40828] Connections initialized by the AWS IoT Device SDK v2 for Java (versions prior to 1.3.3), Python (versions prior to 1.5.18), C++ (versions prior to 1.12.7) and Node.js (versions prior to 1.5.1) did not verify server certificate hostname during TLS handshake when overriding Certificate Authorities (CA) in their trust stores on Windows. This issue has been addressed in aws-c-io submodule versions 0.9.13 onward. This issue affects: Amazon Web Services AWS IoT Device SDK v2 for Java versions prior to 1.3.3 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Python versions prior to 1.5.18 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for C++ versions prior to 1.12.7 on Microsoft Windows. Amazon Web Services AWS IoT Device SDK v2 for Node.js versions prior to 1.5.3 on Microsoft Windows.  
  
[CVE-2021-41065] An issue was discovered in Listary through 6. An attacker can create a \\.\pipe\Listary.listaryService named pipe and wait for a privileged user to open a session on the Listary installed host. Listary will automatically access the named pipe and the attacker will be able to duplicate the victim's token to impersonate him. This exploit is valid in certain Windows versions (Microsoft has patched the issue in later Windows 10 builds).  
  
[CVE-2021-41330] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2021-42275] Microsoft COM for Windows Remote Code Execution Vulnerability  
  
[CVE-2021-42276] Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
  
[CVE-2022-1794] The CODESYS OPC DA Server prior V3.5.18.20 stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system.  
  
[CVE-2022-21606] Vulnerability in the Oracle Services for Microsoft Transaction Server component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Services for Microsoft Transaction Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Services for Microsoft Transaction Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Services for Microsoft Transaction Server accessible data as well as unauthorized read access to a subset of Oracle Services for Microsoft Transaction Server accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).  
  
[CVE-2022-21993] Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability  
  
[CVE-2022-22516] The SysDrv3S driver in the CODESYS Control runtime system on Microsoft Windows allows any system user to read and write within restricted memory space.  
  
[CVE-2022-22765] BD Viper LT system, versions 2.0 and later, contains hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). BD Viper LT system versions 4.0 and later utilize Microsoft Windows 10 and have additional Operating System hardening configurations which increase the attack complexity required to exploit this vulnerability.  
  
[CVE-2022-22782] "The Zoom Client for Meetings for Windows prior to version 5.9.7, Zoom Rooms for Conference Room for Windows prior to version 5.10.0, Zoom Plugins for Microsoft Outlook for Windows prior to version 5.10.3, and Zoom VDI Windows Meeting Clients prior to version 5.9.6  
[CVE-2022-23235] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.10P1 are susceptible to a vulnerability which could allow an attacker to discover cluster, node and Active IQ Unified Manager specific information via AutoSupport telemetry data that is sent even when AutoSupport has been disabled.  
  
[CVE-2022-23239] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows administrative users to perform a Stored Cross-Site Scripting (XSS) attack.  
  
[CVE-2022-23240] Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.11P1 are susceptible to a vulnerability which allows unauthorized users to update EMS Subscriptions via unspecified vectors.  
  
[CVE-2022-23609] iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible.  
  
[CVE-2022-23611] iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdcd48b. Users are advised to upgrade.  
  
[CVE-2022-23678] A vulnerability in the Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system client communications that could allow for an attacker in a privileged network position to intercept sensitive information in Aruba Virtual Intranet Access (VIA) client for Microsoft Windows operating system versions: 4.3.0 build 2208101 and below. Aruba has released upgrades for Virtual Intranet Access (VIA) Client that address this security vulnerability.  
  
[CVE-2022-24765] Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder `C:\.git`, which would be picked up by Git operations run supposedly outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash users who set `GIT\_PS1\_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-gitare vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config`. Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access from those folders as a workaround. Alternatively, define or extend `GIT\_CEILING\_DIRECTORIES` to cover the \_parent\_ directory of the user profile, e.g. `C:\Users` if the user profile is located in `C:\Users\my-user-name`.  
  
[CVE-2022-24826] On Windows, if Git LFS operates on a malicious repository with a `..exe` file as well as a file named `git.exe`, and `git.exe` is not found in `PATH`, the `..exe` program will be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. Similarly, if the malicious repository contains files named `..exe` and `cygpath.exe`, and `cygpath.exe` is not found in `PATH`, the `..exe` program will be executed when certain Git LFS commands are run. More generally, if the current working directory contains any file with a base name of `.` and a file extension from `PATHEXT` (except `.bat` and `.cmd`), and also contains another file with the same base name as a program Git LFS intends to execute (such as `git`, `cygpath`, or `uname`) and any file extension from `PATHEXT` (including `.bat` and `.cmd`), then, on Windows, when Git LFS attempts to execute the intended program the `..exe`, `..com`, etc., file will be executed instead, but only if the intended program is not found in any directory listed in `PATH`. The vulnerability occurs because when Git LFS detects that the program it intends to run does not exist in any directory listed in `PATH` then Git LFS passes an empty string as the executable file path to the Go `os/exec` package, which contains a bug such that, on Windows, it prepends the name of the current working directory (i.e., `.`) to the empty string without adding a path separator, and as a result searches in that directory for a file with the base name `.` combined with any file extension from `PATHEXT`, executing the first one it finds. (The reason `..bat` and `..cmd` files are not executed in the same manner is that, although the Go `os/exec` package tries to execute them just as it does a `..exe` file, the Microsoft Win32 API `CreateProcess()` family of functions have an undocumented feature in that they apparently recognize when a caller is attempting to execute a batch script file and instead run the `cmd.exe` command interpreter, passing the full set of command line arguments as parameters. These are unchanged from the command line arguments set by Git LFS, and as such, the intended program's name is the first, resulting in a command line like `cmd.exe /c git`, which then fails.) Git LFS has resolved this vulnerability by always reporting an error when a program is not found in any directory listed in `PATH` rather than passing an empty string to the Go `os/exec` package in this case. The bug in the Go `os/exec` package has been reported to the Go project and is expected to be patched after this security advisory is published. The problem was introduced in version 2.12.1 and is patched in version 3.1.3. Users of affected versions should upgrade to version 3.1.3. There are currently no known workarounds at this time.  
  
[CVE-2022-27167] "Privilege escalation vulnerability in Windows products of ESET, spol. s r.o. allows attacker to exploit ""Repair"" and ""Uninstall"" features what may lead to arbitrary file deletion. This issue affects: ESET, spol. s r.o. ESET NOD32 Antivirus 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Internet Security 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Smart Security Premium 11.2 versions prior to 15.1.12.0. ESET, spol. s r.o. ESET Endpoint Antivirus 6.0 versions prior to 9.0.2046.0. ESET, spol. s r.o. ESET Endpoint Security 6.0 versions prior to 9.0.2046.0. ESET, spol. s r.o. ESET Server Security for Microsoft Windows Server 8.0 versions prior to 9.0.12012.0. ESET, spol. s r.o. ESET File Security for Microsoft Windows Server 8.0.12013.0. ESET, spol. s r.o. ESET Mail Security for Microsoft Exchange Server 6.0 versions prior to 8.0.10020.0. ESET, spol. s r.o. ESET Mail Security for IBM Domino 6.0 versions prior to 8.0.14011.0. ESET, spol. s r.o. ESET Security for Microsoft SharePoint Server 6.0 versions prior to 8.0.15009.0."  
  
[CVE-2022-27608] Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows is vulnerable to registry key tampering by users with Administrator privileges. This could result in a user disabling anti-tampering mechanisms which would then allow the user to disable Forcepoint One Endpoint and the protection offered by it.  
  
[CVE-2022-27609] Forcepoint One Endpoint prior to version 22.01 installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling Forcepoint One Endpoint and the protection offered by it.  
  
[CVE-2022-29105] Microsoft Windows Media Foundation Remote Code Execution Vulnerability.  
  
[CVE-2022-30190] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.  
  
[CVE-2022-32230] Microsoft Windows SMBv3 suffers from a null pointer dereference in versions of Windows prior to the April, 2022 patch set. By sending a malformed FileNormalizedNameInformation SMBv3 request over a named pipe, an attacker can cause a Blue Screen of Death (BSOD) crash of the Windows kernel. For most systems, this attack requires authentication, except in the special case of Windows Domain Controllers, where unauthenticated users can always open named pipes as long as they can establish an SMB session. Typically, after the BSOD, the victim SMBv3 server will reboot.  
  
[CVE-2022-34006] An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. When installing, Microsoft SQL Express 2019 installs by default with an SQL instance running as SYSTEM with BUILTIN\Users as sysadmin, thus enabling unprivileged Windows users to execute commands locally as NT AUTHORITY\SYSTEM, aka NX-I674 (sub-issue 2). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation.  
  
[CVE-2022-34478] The <code>ms-msdt</code>, <code>search</code>, and <code>search-ms</code> protocols deliver content to Microsoft applications, bypassing the browser, when a user accepts a prompt. These applications have had known vulnerabilities, exploited in the wild (although we know of none exploited through Thunderbird), so in this release Thunderbird has blocked these protocols from prompting the user to open them.<br>\*This bug only affects Thunderbird on Windows. Other operating systems are unaffected.\*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.  
  
[CVE-2022-34713] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability  
  
[CVE-2022-35743] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability  
  
[CVE-2022-36670] PCProtect Endpoint prior to v5.17.470 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.  
  
[CVE-2022-37771] IObit Malware Fighter v9.2 for Microsoft Windows lacks tamper protection, allowing authenticated attackers with Administrator privileges to modify processes within the application and escalate privileges to SYSTEM via a crafted executable.  
  
[CVE-2022-37971] Microsoft Windows Defender Elevation of Privilege Vulnerability.  
  
[CVE-2022-39327] Azure CLI is the command-line interface for Microsoft Azure. In versions previous to 2.40.0, Azure CLI contains a vulnerability for potential code injection. Critical scenarios are where a hosting machine runs an Azure CLI command where parameter values have been provided by an external source. The vulnerability is only applicable when the Azure CLI command is run on a Windows machine and with any version of PowerShell and when the parameter value contains the `&` or `|` symbols. If any of these prerequisites are not met, this vulnerability is not applicable. Users should upgrade to version 2.40.0 or greater to receive a a mitigation for the vulnerability.  
  
[CVE-2022-40263] BD Totalys MultiProcessor, versions 1.70 and earlier, contain hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). Customers using BD Totalys MultiProcessor version 1.70 with Microsoft Windows 10 have additional operating system hardening configurations which increase the attack complexity required to exploit this vulnerability.  
  
[CVE-2022-41120] Microsoft Windows System Monitor (Sysmon) Elevation of Privilege Vulnerability  
  
[CVE-2022-44704] Microsoft Windows Sysmon Elevation of Privilege Vulnerability.  
  
[CVE-2022-45141] Since the Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96).  
  
[CVE-2023-1587] Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The issue was fixed with Avast and AVG Antivirus version 22.11  
  
[CVE-2023-22880] "Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft&#8217  
[CVE-2023-28005] "A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows&#65533  
[CVE-2023-28290] Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability  
  
[CVE-2023-28297] Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability  
  
[CVE-2023-31222] "Deserialization of untrusted data in Microsoft Messaging Queuing Service in Medtronic's Paceart Optima versions 1.11 and earlier on Windows allows an unauthorized user to impact a healthcare delivery organization&#8217  
[CVE-2023-34355] Uncontrolled search path element for some Intel(R) Server Board M10JNP2SB integrated BMC video drivers before version 3.0 for Microsoft Windows and before version 1.13.4 for linux may allow an authenticated user to potentially enable escalation of privilege via local access.  
  
[CVE-2023-38175] Microsoft Windows Defender Elevation of Privilege Vulnerability  
  
[CVE-2023-38402] A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow malicious users to overwrite arbitrary files as NT AUTHORITY\SYSTEM. A successful exploit could allow these malicious users to create a Denial-of-Service (DoS) condition affecting the Microsoft Windows operating System boot process.

### Узел 192.168.233.131/24

Состояние: up

Количество открытых портов: 2

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |
| 8000 | open | syn-ack | http-alt |  |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.  
  
  
  
Emptys

### Узел 192.168.233.254/24

Состояние: up

Количество открытых портов: 0

Общее количество CVE: 0

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |

#### Описание CVE: