Vulnerabilities Report

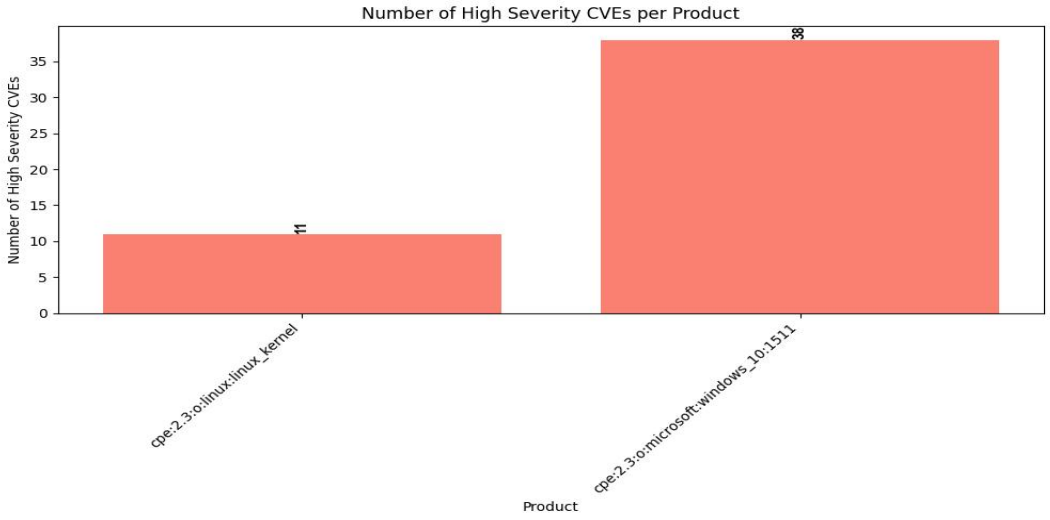
*Total CVEs Analyzed: 100
*Total Affected Products: 2
*Product with Most CVEs:
cpe:2.3:o:linux:linux_kernel

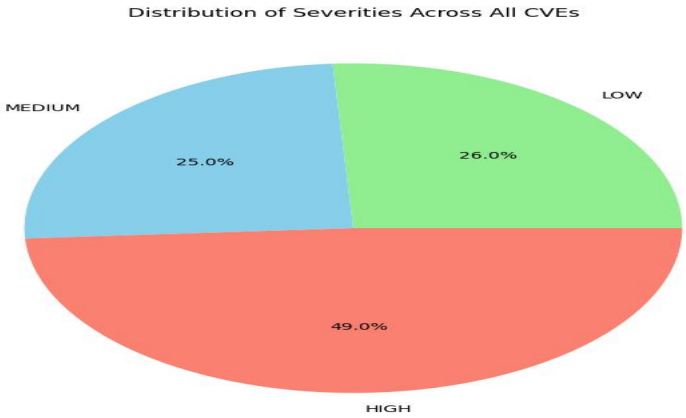
*CVEs per Product Count:
- cpe:2.3:o:linux:linux_kernel: 50
- cpe:2.3:o:microsoft:windows_10:1511: 50

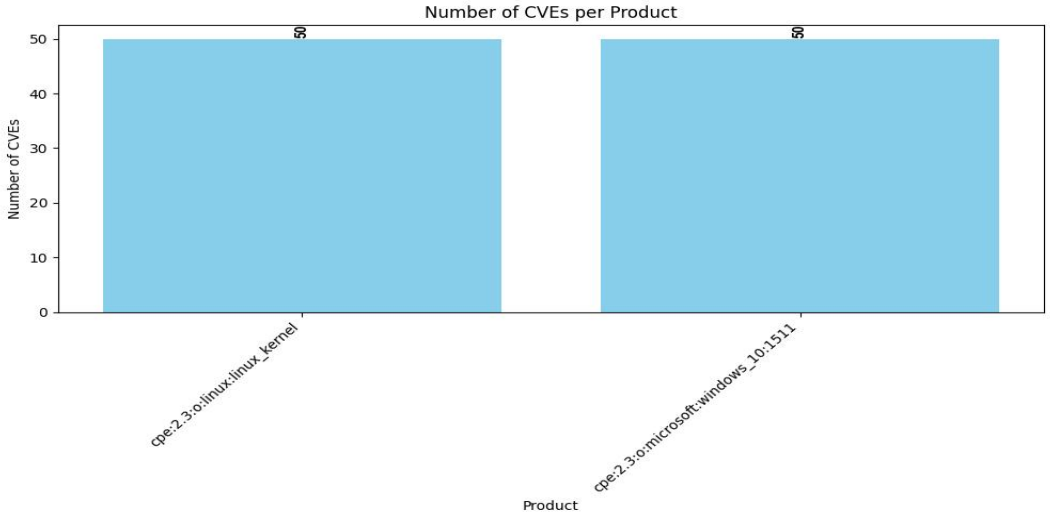
*Severity Distribution Across All CVEs:
- LOW: 26
- MEDIUM: 25
- HIGH: 49

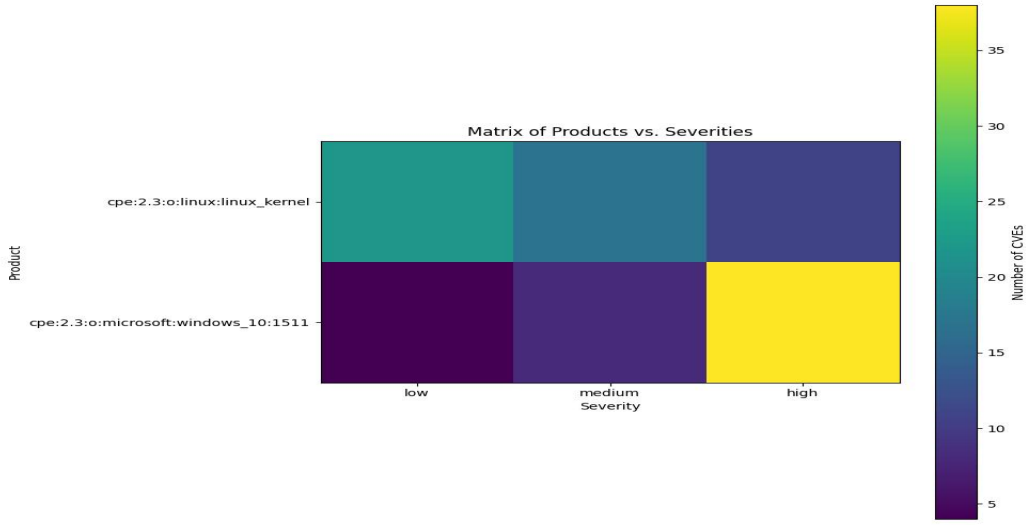
*Severity Distribution Per Product:
cpe:2.3:o:linux:linux_kernel:
- low: 22
- medium: 17
- high: 11

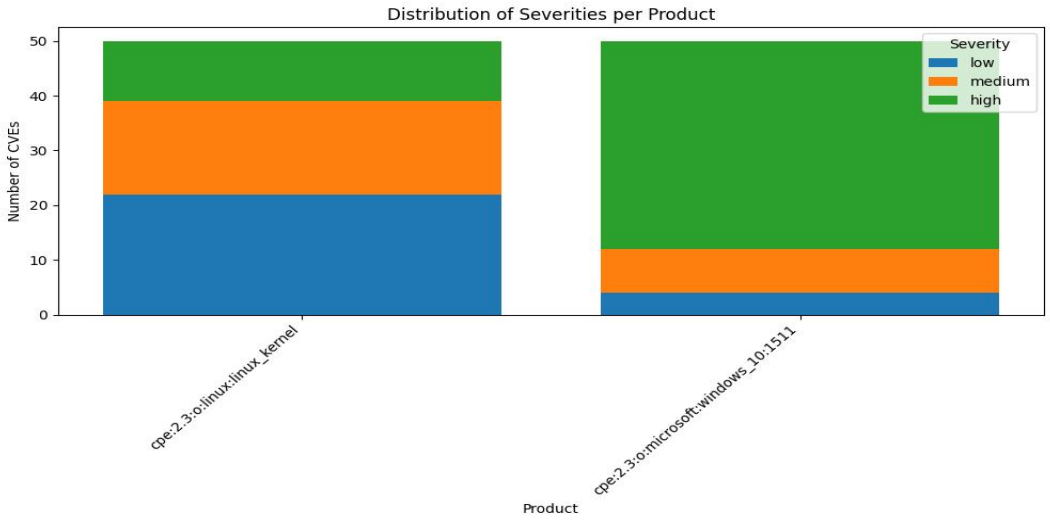
cpe:2.3:o:microsoft:windows_10:1511:
- low: 4
- medium: 8
- high: 38




Distribution of Severities Across All CVEs
MEDIUM
LOW
25.0%
26.0%
49.0%
HIGH


Number of CVEs per Product
Number of CVEs
50
50
0
10
20
30
40
50
cpe:2.3:o:linux:linux_kernel
cpe:2.3:o:microsoft:windows_10:1511
Product


Matrix of Products vs. Severities
Product
cpe:2.3:o:linux:linux_kernel
cpe:2.3:o:microsoft:windows_10:1511
low
medium
high
Severity
Number of CVEs
5
10
15
20
25
30
35



*Detailed CVES data per product: cpe:2.3:o:linux:linux_kernel

{'CVE ID': 'CVE-1999-0138', 'Base Severity': 'HIGH', 'Last Modified': '2022-08-17T07:15:11.853', 'Description': 'The suidperl and sperl program do not give up root privileges when changing UIDs back to the original users, allowing root access.', 'Base Score': 7.2}
{'CVE ID': 'CVE-1999-0128', 'Base Severity': 'MEDIUM', 'Last Modified': '2022-08-17T07:15:11.577', 'Description': "Oversized ICMP ping packets can result in a denial of service, aka Ping o' Death.", 'Base Score': 5.0}
{'CVE ID': 'CVE-1999-0513', 'Base Severity': 'MEDIUM', 'Last Modified': '2022-08-17T08:15:13.503', 'Description': 'ICMP messages to broadcast addresses are allowed, allowing for a Smurf attack that can cause a denial of service.', 'Base Score': 5.0}
{'CVE ID': 'CVE-1999-1442', 'Base Severity': 'HIGH', 'Last Modified': '2018-09-11T18:41:31.247', 'Description': 'Bug in AMD K6 processor on Linux 2.0.x and 2.1.x kernels allows local users to cause a denial of service (crash) via a particular sequence of instructions, possibly related to accessing addresses outside of segments.', 'Base Score': 7.2}
{'CVE ID': 'CVE-1999-1441', 'Base Severity': 'LOW', 'Last Modified': '2016-10-18T02:04:36.803', 'Description': 'Linux 2.0.34 does not properly prevent users from sending SIGIO signals to arbitrary processes, which allows local users to cause a denial of service by sending SIGIO to processes that do not catch it.', 'Base Score': 2.1}
{'CVE ID': 'CVE-1999-1285', 'Base Severity': 'LOW', 'Last Modified': '2017-12-19T02:29:07.190', 'Description': 'Linux 2.1.132 and earlier allows local users to cause a denial of service (resource exhaustion) by reading a large buffer from a random device (e.g. /dev/urandom), which cannot be interrupted until the read has completed.', 'Base Score': 2.1}
{'CVE ID': 'CVE-1999-0401', 'Base Severity': 'LOW', 'Last Modified': '2022-08-17T08:15:11.327', 'Description': 'A race condition in Linux 2.2.1 allows local users to read arbitrary memory from /proc files.', 'Base Score': 3.7}
{'CVE ID': 'CVE-1999-0451', 'Base Severity': 'LOW', 'Last Modified': '2008-09-05T20:17:18.560', 'Description': 'Denial of service in Linux 2.0.36 allows local users to prevent any server from listening on any non-privileged port.', 'Base Score': 2.1}
{'CVE ID': 'CVE-1999-0400', 'Base Severity': 'MEDIUM', 'Last Modified': '2008-09-05T20:17:11.140', 'Description': 'Denial of service in Linux 2.2.0 running the ldd command on a core file.', 'Base Score': 4.6}
{'CVE ID': 'CVE-1999-0460', 'Base Severity': 'LOW', 'Last Modified': '2008-09-05T20:17:19.560', 'Description': 'Buffer overflow in Linux autofs module through long directory names allows local users to perform a denial of service.', 'Base Score': 2.1}
{'CVE ID': 'CVE-1999-0414', 'Base Severity': 'MEDIUM', 'Last Modified': '2022-08-17T08:15:11.620',

'Description': 'In Linux before version 2.0.36, remote attackers can spoof a TCP connection and pass data to the application layer before fully establishing the connection.', 'Base Score': 5.0}
{'CVE ID': 'CVE-1999-0431', 'Base Severity': 'MEDIUM', 'Last Modified': '2022-08-17T08:15:12.063', 'Description': 'Linux 2.2.3 and earlier allow a remote attacker to perform an IP fragmentation attack, causing a denial of service.', 'Base Score': 5.0}
{'CVE ID': 'CVE-1999-0804', 'Base Severity': 'MEDIUM', 'Last Modified': '2008-09-09T12:35:40.307', 'Description': 'Denial of service in Linux 2.2.x kernels via malformed ICMP packets containing unusual types, codes, and IP header lengths.', 'Base Score': 5.0}
{'CVE ID': 'CVE-1999-1166', 'Base Severity': 'HIGH', 'Last Modified': '2008-09-05T20:18:52.680', 'Description': 'Linux 2.0.37 does not properly encode the Custom segment limit, which allows local users to gain root privileges by accessing and modifying kernel memory.', 'Base Score': 7.2}
{'CVE ID': 'CVE-1999-1018', 'Base Severity': 'HIGH', 'Last Modified': '2016-10-18T02:00:16.213', 'Description': 'IPChains in Linux kernels 2.2.10 and earlier does not reassemble IP fragments before checking the header information, which allows a remote attacker to bypass the filtering rules using several fragments with 0 offsets.', 'Base Score': 7.5}
{'CVE ID': 'CVE-1999-1352', 'Base Severity': 'MEDIUM', 'Last Modified': '2016-10-18T02:03:24.073', 'Description': 'mknod in Linux 2.2 follows symbolic links, which could allow local users to overwrite files or gain privileges.', 'Base Score': 4.6}
{'CVE ID': 'CVE-1999-1341', 'Base Severity': 'MEDIUM', 'Last Modified': '2018-09-11T14:32:55.857', 'Description': 'Linux kernel before 2.3.18 or 2.2.13pre15, with SLIP and PPP options, allows local unprivileged users to forge IP packets via the TIOCSETD option on tty devices.', 'Base Score': 4.6}
{'CVE ID': 'CVE-1999-0986', 'Base Severity': 'MEDIUM', 'Last Modified': '2008-09-09T12:36:35.447', 'Description': 'The ping command in Linux 2.0.3x allows local users to cause a denial of service by sending large packets with the -R (record route) option.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2000-0006', 'Base Severity': 'LOW', 'Last Modified': '2017-10-10T01:29:06.997', 'Description': 'strace allows local users to read arbitrary files via memory mapped file names.', 'Base Score': 2.6}
{'CVE ID': 'CVE-1999-1339', 'Base Severity': 'MEDIUM', 'Last Modified': '2016-10-18T02:03:07.960', 'Description': 'Vulnerability when Network Address Translation (NAT) is enabled in Linux 2.2.10 and earlier with ipchains, or FreeBSD 3.2 with ipfw, allows remote attackers to cause a denial of service (kernel panic) via a ping -R (record route) command.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2000-0227', 'Base Severity': 'LOW', 'Last Modified': '2017-12-20T02:29:00.317', 'Description': 'The Linux 2.2.x kernel does not restrict the number of Unix domain sockets as defined by the wmem_max parameter, which allows local users to cause a denial of service by requesting a large number of sockets.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2000-0289', 'Base Severity': 'MEDIUM', 'Last Modified': '2008-09-10T19:04:00.557', 'Description': 'IP masquerading in Linux 2.2.x allows remote attackers to route UDP packets through the internal interface by modifying the external source IP address and port number to match those of an established connection.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2000-0344', 'Base Severity': 'MEDIUM', 'Last Modified': '2023-11-07T01:55:17.297', 'Description': 'The knfsd NFS server in Linux kernel 2.2.x allows remote attackers to cause a denial of service via a negative size value.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2000-0506', 'Base Severity': 'HIGH', 'Last Modified': '2023-11-07T01:55:19.603', 'Description': 'The "capabilities" feature in Linux before 2.2.16 allows local users to cause a denial of service or gain privileges by setting the capabilities to prevent a setuid program from dropping privileges, aka the "Linux kernel setuid/setcap vulnerability."', 'Base Score': 10.0}
{'CVE ID': 'CVE-2001-1273', 'Base Severity': 'LOW', 'Last Modified': '2008-09-05T20:26:07.687', 'Description': 'The "mxcsr P4" vulnerability in the Linux kernel before 2.2.17-14, when running on certain Intel CPUs, allows local users to cause a denial of service (system halt).', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1390', 'Base Severity': 'MEDIUM', 'Last Modified': '2016-12-08T02:59:05.767', 'Description': 'Unknown vulnerability in binfmt_misc in the Linux kernel before 2.2.19, related to user pages.', 'Base Score': 6.2}
{'CVE ID': 'CVE-2001-1391', 'Base Severity': 'LOW', 'Last Modified': '2024-02-02T02:56:22.740',

'Description': 'Off-by-one vulnerability in CPIA driver of Linux kernel before 2.2.19 allows users to modify kernel memory.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1392', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:08.140', 'Description': 'The Linux kernel before 2.2.19 does not have unregister calls for (1) CPUID and (2) MSR drivers, which could cause a DoS (crash) by unloading and reloading the drivers.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1393', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:09.187', 'Description': 'Unknown vulnerability in classifier code for Linux kernel before 2.2.19 could result in denial of service (hang).', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1394', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:10.330', 'Description': 'Signedness error in (1) getsockopt and (2) setsockopt for Linux kernel before 2.2.19 allows local users to cause a denial of service.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1395', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:11.517', 'Description': 'Unknown vulnerability in sockfilter for Linux kernel before 2.2.19 related to "boundary cases," with unknown impact.', 'Base Score': 3.6}
{'CVE ID': 'CVE-2001-1396', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:12.563', 'Description': 'Unknown vulnerabilities in strnlen_user for Linux kernel before 2.2.19, with unknown impact.', 'Base Score': 3.6}
{'CVE ID': 'CVE-2001-1397', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:13.703', 'Description': 'The System V (SYS5) shared memory implementation for Linux kernel before 2.2.19 could allow attackers to modify recently freed memory.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1398', 'Base Severity': 'HIGH', 'Last Modified': '2016-12-08T02:59:14.737', 'Description': 'Masquerading code for Linux kernel before 2.2.19 does not fully check packet lengths in certain cases, which may lead to a vulnerability.', 'Base Score': 7.5}
{'CVE ID': 'CVE-2001-1399', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:15.813', 'Description': 'Certain operations in Linux kernel before 2.2.19 on the x86 architecture copy the wrong number of bytes, which might allow attackers to modify memory, aka "User access asm bug on x86."', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1400', 'Base Severity': 'LOW', 'Last Modified': '2016-12-08T02:59:16.907', 'Description': 'Unknown vulnerabilities in the UDP port allocation for Linux kernel before 2.2.19 could allow local users to cause a denial of service (deadlock).', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-0316', 'Base Severity': 'MEDIUM', 'Last Modified': '2017-10-10T01:29:40.640', 'Description': 'Linux kernel 2.4 and 2.2 allows local users to read kernel memory and possibly gain privileges via a negative argument to the sysctl call.', 'Base Score': 4.6}
{'CVE ID': 'CVE-2001-0317', 'Base Severity': 'LOW', 'Last Modified': '2017-10-10T01:29:40.687', 'Description': 'Race condition in ptrace in Linux kernel 2.4 and 2.2 allows local users to gain privileges by using ptrace to track and modify a running setuid process.', 'Base Score': 3.7}
{'CVE ID': 'CVE-2001-0405', 'Base Severity': 'HIGH', 'Last Modified': '2017-10-10T01:29:42.890', 'Description': 'ip_conntrack_ftp in the IPTables firewall for Linux 2.4 allows remote attackers to bypass access restrictions for an FTP server via a PORT command that lists an arbitrary IP address and port number, which is added to the RELATED table and allowed by the firewall.', 'Base Score': 7.5}
{'CVE ID': 'CVE-2001-1244', 'Base Severity': 'MEDIUM', 'Last Modified': '2018-10-30T16:26:22.763', 'Description': 'Multiple TCP implementations could allow remote attackers to cause a denial of service (bandwidth and CPU exhaustion) by setting the maximum segment size (MSS) to a very small number and requesting large amounts of data, which generates more packets with less TCP-level data that amplify network traffic and consume more server CPU to process.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2001-1056', 'Base Severity': 'HIGH', 'Last Modified': '2018-09-20T18:45:46.970', 'Description': 'IRC DCC helper in the ip_masq_irc IP masquerading module 2.2 allows remote attackers to bypass intended firewall restrictions by causing the target system to send a "DCC SEND" request to a malicious server which listens on port 6667, which may cause the module to believe that the traffic is a valid request and allow the connection to the port specified in the DCC SEND request.', 'Base Score': 7.5}
{'CVE ID': 'CVE-2001-0907', 'Base Severity': 'LOW', 'Last Modified': '2018-09-20T18:45:41.923', 'Description': 'Linux kernel 2.2.1 through 2.2.19, and 2.4.1 through 2.4.10, allows local users to cause a

denial of service via a series of deeply nested symlinks, which causes the kernel to spend extra time when trying to access the link.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1384', 'Base Severity': 'HIGH', 'Last Modified': '2016-10-18T02:14:49.437', 'Description': 'ptrace in Linux 2.2.x through 2.2.19, and 2.4.x through 2.4.9, allows local users to gain root privileges by running ptrace on a setuid or setgid program that itself calls an unprivileged program, such as newgrp.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2001-0914', 'Base Severity': 'LOW', 'Last Modified': '2017-10-10T01:29:56.343', 'Description': 'Linux kernel before 2.4.11pre3 in multiple Linux distributions allows local users to cause a denial of service (crash) by starting the core vmlinux kernel, possibly related to poor error checking during ELF loading.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-0851', 'Base Severity': 'MEDIUM', 'Last Modified': '2017-10-10T01:29:54.423', 'Description': 'Linux kernel 2.0, 2.2 and 2.4 with syncookies enabled allows remote attackers to bypass firewall rules by brute force guessing the cookie.', 'Base Score': 5.0}
{'CVE ID': 'CVE-2001-1551', 'Base Severity': 'LOW', 'Last Modified': '2008-09-05T20:26:50.450', 'Description': 'Linux kernel 2.2.19 enables CAP_SYS_RESOURCE for setuid processes, which allows local users to exceed disk quota restrictions during execution of setuid programs.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2001-1572', 'Base Severity': 'HIGH', 'Last Modified': '2008-09-05T20:26:53.560', 'Description': 'The MAC module in Netfilter in Linux kernel 2.4.1 through 2.4.11, when configured to filter based on MAC addresses, allows remote attackers to bypass packet filters via small packets.', 'Base Score': 7.5}
{'CVE ID': 'CVE-2002-0060', 'Base Severity': 'HIGH', 'Last Modified': '2017-10-10T01:30:04.733', 'Description': 'IRC connection tracking helper module in the netfilter subsystem for Linux 2.4.18-pre9 and earlier does not properly set the mask for conntrack expectations for incoming DCC connections, which could allow remote attackers to bypass intended firewall restrictions.', 'Base Score': 7.5}
{'CVE ID': 'CVE-2002-0570', 'Base Severity': 'LOW', 'Last Modified': '2017-12-19T02:29:37.893', 'Description': 'The encrypted loop device in Linux kernel 2.4.10 and earlier does not authenticate the entity that is encrypting data, which allows local users to modify encrypted data without knowing the key.', 'Base Score': 2.1}
{'CVE ID': 'CVE-2002-0704', 'Base Severity': 'MEDIUM', 'Last Modified': '2024-02-03T02:31:30.647', 'Description': 'The Network Address Translation (NAT) capability for Netfilter ("iptables") 1.2.6a and earlier leaks translated IP addresses in ICMP error messages.', 'Base Score': 5.0}

cpe:2.3:o:microsoft:windows_10:1511

{'CVE ID': 'CVE-2015-2478', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T13:04:02.360', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6095', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-17T12:11:17.420', 'Description': '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."', 'Base Score': 4.9}
{'CVE ID': 'CVE-2015-6100', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-15T12:42:18.103', 'Description': '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.', 'Base Score': 6.9}
{'CVE ID': 'CVE-2015-6101', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-15T13:32:03.030', 'Description': '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.', 'Base Score': 6.9}
{'CVE ID': 'CVE-2015-6102', 'Base Severity': 'LOW', 'Last Modified': '2019-05-16T19:38:25.110', 'Description': '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."', 'Base Score': 2.1}
{'CVE ID': 'CVE-2015-6103', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-17T19:19:24.780', 'Description': '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.', 'Base Score': 9.3}
{'CVE ID': 'CVE-2015-6104', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-17T20:01:11.033', 'Description': '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.', 'Base Score': 9.3}
{'CVE ID': 'CVE-2015-6109', 'Base Severity': 'LOW', 'Last Modified': '2019-05-15T14:48:18.130', 'Description': '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."', 'Base Score': 2.1}
{'CVE ID': 'CVE-2015-6113', 'Base Severity': 'LOW', 'Last Modified': '2019-05-16T18:48:12.883', 'Description': '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."', 'Base Score': 2.1}
{'CVE ID': 'CVE-2015-6107', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T14:39:57.263', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2015-6126', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-16T19:06:41.817', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6132', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T19:24:52.627', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6133', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T13:59:50.003',

'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6171', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T15:07:57.317', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6173', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T15:09:51.853', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2015-6174', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T15:31:23.057', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0006', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-17T20:08:17.717', 'Description': '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.', 'Base Score': 6.9}
{'CVE ID': 'CVE-2016-0007', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-17T20:17:51.557', 'Description': '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.', 'Base Score': 6.9}
{'CVE ID': 'CVE-2016-0009', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-30T16:27:22.263', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0014', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-16T18:24:13.693', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0015', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-17T19:13:58.827', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0016', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T14:36:07.040', 'Description': '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."', 'Base Score': 7.2}

{'CVE ID': 'CVE-2016-0018', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-05-15T18:59:47.013', 'Description': '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."', 'Base Score': 6.9}
{'CVE ID': 'CVE-2016-0019', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-30T16:27:22.263', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0038', 'Base Severity': 'HIGH', 'Last Modified': '2019-05-15T15:08:31.960', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0041', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:10:50.393', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0042', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:10:50.970', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0048', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:10:51.817', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0049', 'Base Severity': 'LOW', 'Last Modified': '2018-10-30T16:27:22.200', 'Description': '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."', 'Base Score': 2.1}
{'CVE ID': 'CVE-2016-0051', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:10:52.627', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0091', 'Base Severity': 'MEDIUM', 'Last Modified': '2018-10-12T22:11:01.427', 'Description': '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.', 'Base Score': 6.8}
{'CVE ID': 'CVE-2016-0092', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:01.783', 'Description': '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.', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0093', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:02.223',

'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0094', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:02.567', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0095', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:02.910', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0096', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:03.237', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0099', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:03.800', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0101', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:04.690', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0117', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:10.677', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0118', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:10.940', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0120', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:11.270', 'Description': '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."', 'Base Score': 7.1}
{'CVE ID': 'CVE-2016-0121', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:11.597', 'Description': '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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0133', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:14.817',

'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0128', 'Base Severity': 'MEDIUM', 'Last Modified': '2019-09-27T17:21:55.877', 'Description': '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."', 'Base Score': 5.8}
{'CVE ID': 'CVE-2016-0135', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:15.427', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0143', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:17.503', 'Description': '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.', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0145', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:17.910', 'Description': 'The 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 and 1511; Office 2007 SP3 and 2010 SP2; Word Viewer; .NET Framework 3.0 SP2, 3.5, and 3.5.1; Skype for Business 2016; Lync 2010; Lync 2010 Attendee; 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."', 'Base Score': 9.3}
{'CVE ID': 'CVE-2016-0150', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:19.537', 'Description': '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."', 'Base Score': 7.8}
{'CVE ID': 'CVE-2016-0151', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:19.723', 'Description': '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."', 'Base Score': 7.2}
{'CVE ID': 'CVE-2016-0165', 'Base Severity': 'HIGH', 'Last Modified': '2018-10-12T22:11:23.287', 'Description': '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.', 'Base Score': 7.2}