CVE IDs	Vulnerability Description
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-2016-3309	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-2016-3308, CVE-2016-3310, and CVE-2016-3311.
CVE-2017-0101	The kernel-mode drivers in Transaction Manager in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2; 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 "Windows Elevation of Privilege Vulnerability.
CVE-2018-8120	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows Server 2008, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8124, CVE-2018-8164, CVE-2018-8166.
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-2019-0841	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836.
CVE-2019-1064	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'.
CVE-2019-1069	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations, aka 'Task Scheduler Elevation of Privilege Vulnerability'.
CVE-2019-1129	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1130.
CVE-2019-1130	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1129.
CVE-2019-1215	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303.
CVE-2019-1253	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1278, CVE-2019-1303.

infinitum IT
Power of integrated Security
https://www.infinitumit.com.tr/

CVE-2019-1315	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.							
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-2019-1385	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'.							
CVE-2019-1388	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'.							
CVE-2019-1405	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'.							
CVE-2019-1458	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.							
CVE-2020-0609	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0610.							
CVE-2020-0638	An elevation of privilege vulnerability exists in the way the Update Notification Manager handles files.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Update Notification Manager Elevation of Privilege Vulnerability'.							
CVE-2020-0688	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.							
CVE-2020-0787	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) improperly handles symbolic links, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.							
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-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.							
CVE-2021-1675	Windows Print Spooler Elevation of Privilege Vulnerability							
CVE-2021-1732	Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1698.							
CVE-2021-21972	The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).							

CVE-2021-21985	The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.							
CVE-2021-22005	The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file.							
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078.							
CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability							
CVE-2021-44847	A stack-based buffer overflow in handle_request function in DHT.c in toxcore 0.1.9 through 0.1.11 and 0.2.0 through 0.2.12 (caused by an improper length calculation during the handling of received network packets) allows remote attackers to crash the process or potentially execute arbitrary code via a network packet.							