PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Edge Remote Chakra Scripting Engine Memory Corruption Vulnerability - CVE-2017-0223	Microsoft Edge Remote Chakra Scripting Engine Memory Corruption Vulnerability - CVE-2017-0223 The Chakra JavaScript engine in Microsoft Edge on Windows 10 version 1703, does not properly render when handling objects in memory, making it prone to a remote code execution vulnerability. A remote attacker could exploit this issue to cause memory corruption and execute arbitrary code in the context of the current user. To exploit this issue the attacker would have to entice the victim to visit a maliciously crafted web site or to open a maliciously crafted file.	Version(s): <=Windows Ver 10.	Published - May 12, 2017 CVE-2017-0223 CVSS - 7.5 Vendor's Advisory - https://www.microsoft.com/en-us/windows/microsoft-edge http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0223
Linux Kernel 4.11.1 and Earlier Local DoS or Other Impact due to Use-After-Free Error - CVE-2017-7487	Linux Kernel 4.11.1 and Earlier Local DoS or Other Impact due to Use-After-Free Error - CVE-2017-7487 The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.	Version(s): <=4.11.1	Published - May 12, 2017 CVE-CVE-2017-7487 CVSS - 7.2 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7487
Microsoft Dxgkrnl.sys Elevation of Privilege Vulnerability - CVE-2017-0077	Microsoft Dxgkrnl.sys Elevation of Privilege Vulnerability - CVE-2017-0077 The Microsoft DirectX graphics kernel subsystem (Dxgkrnl.sys) in the kernel-mode drivers in Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10 and Windows Server 2016 is prone to an elevation of privileges vulnerability. A local attacker could exploit the flaw via a crafted application in order to run processes in an elevated context. Also this vulnerability can lead to denial of service on systems with Windows 8.1 or later installed.	Version(s): <=Windows 7,2008 R2, Windows 8, Windows Server 2016, 2008, 2012, 2012 R2, 10	Published - May 09, 2017 CVE-2017-0077 CVSS - 5.6 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0077 https://portal.msrc.microsoft.com/en-us/security-guidance
Microsoft Windows COM Elevation of Privilege Vulnerability - CVE-2017-0214	Microsoft Windows COM Elevation of Privilege Vulnerability - CVE-2017-0214 Microsoft Windows 7, Windows 8.1 and Windows 10, Windows 10 1607, Windows 10 1511 and Windows 10 1703, Windows Server 2008, 2008 R2, 2012, 2012 R2 and Server 2016 are prone to a privilege escalation vulnerability due to improper input validation. An attacker can exploit this vulnerability by using a malicious application after access a local network.	Version(s): <=Windows 7,2008 R2, Windows 8, Windows Server 2016, 2008, 2012, 2012 R2, 10	Published - May 09, 2017 CVE-CVE-2017-0214 CVSS - 7.2 Vendor's Advisory - http://www.microsoft.com/windows/default.mspx http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0214
Red Hat JBoss Enterprise Application 7 Remote DoS Vulnerability in Websocket Server - CVE-2017-2670	Red Hat JBoss Enterprise Application 7 Remote DoS Vulnerability in Websocket Server - CVE-2017-2670 Websocket server, as used in Red Hat JBoss Enterprise Application 7, is prone to a remote denial-of-service vulnerability due to an infinite loop on every IO thread when performing non-clean TCP close.	Version(s): <= 70 EL6 % & 7.0EL7	Published - May 08, 2017 CVE-CVE-2017-2670 CVSS - 7.8 Vendor's Advisory - https://access.redhat.com/errata/RHSA-2017:1412 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-2670
Red Hat JBoss Enterprise Application 6, 7 Remote File Read Vulnerability in Wildfly Server - CVE-2017-2595	Red Hat JBoss Enterprise Application 6, 7 Remote File Read Vulnerability in Wildfly Server - CVE-2017-2595 Wildfly server, as used in Red Hat JBoss Enterprise Application 6 and 7, is prone to a remote path traversal vulnerability in the log file viewer. A remote authenticated attacker could exploit this issue to read arbitrary files on the system.	Version(s): <= 70 EL6 % & 7.0EL7	Published - June 08, 2017 CVE-CVE-2017-2595 CVSS - 4.0 Vendor's Advisory - https://access.redhat.com/errata/RHSA-2017:1412 https://access.redhat.com/errata/RHSA-2017:1412
VMWare vSphere Data Protection (VDP) Remote Code Execution Vulnerability - CVE-2017-4914	VMWare vSphere Data Protection (VDP) Remote Code Execution Vulnerability - CVE-2017-4914 VMWare vSphere Data Protection (VDP) versions 6.1 - 6.1.3, 5.5.1 - 6.0.4 is prone to a remote code execution vulnerability due to existing deserialization issue.	Version(s): Windows 6.1 - 6.1.3, 5.5.1, 6.0.4	Published - June 09,2017 09, 2017 CVE-2017-0077 CVSS - 5.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4914http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4914
Cisco NAM, MXE and VSM Remote Code Execution via Samba Server - CVE-2017-7494	Cisco NAM, MXE and VSM Remote Code Execution via Samba Server - CVE-2017-7494 Samba Server as used in Cisco Network Analysis Module version 6.2, Cisco Media Experience Engine versions 3.5, 3.5.1 and 3.5.2, and Cisco Video Surveillance Manager versions 7.7, 7.8 and 7.9 are prone to a remote code execution vulnerability due to a flaw in the Samba server.	Version(s): 3.5, 3.5.1, 3.5.2	Published - June 09,2017 09, 2017 CVE-2017-7494 CVSS - 7.5 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7494 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7494