PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Xen <=4.3 Remote Privilege Escalation in Qemu	Xen 4.3 and earlier ,when qemu is used as a device model, allows x86 HVM guest administrators to gain privileges. This issue exists due to a flaw in handling ioport accesses. NOTE: All versions of Xen are vulnerable wjen using Qemu before version 1.6.0.	Version(s):XENProject <=4.3	Published - December 06,2016 CVE-CVE-2016-9637 CVSS - 9.0 Vendor's Advisory Available at : https://access.redhat.com/errata/RHSA-2016:2963
Netgear Multiple R6000, R7000, R8000, and D6000 Routers Remote Code Injection and Execution Vulnerability	Netgear routers R6250 with firmware version before 1.0.4.6, R6400 with firmware version before 1.0.1.18, R6700 with firmware version before 1.0.1.14, R6900 with firmware version before 1.0.1.14, R7000 with firmware version before 1.0.7.6, R7100LG with firmware version before 1.0.0.28, R7300DST with firmware version before 1.0.0.46, R7900 with firmware version before 1.0.1.8, R8000 with firmware version before 1.0.3.26, D6220 with firmware version before 1.0.0.22, and D6400 with firmware version before 1.0.0.56 allow remote attackers to execute arbitrary commands via shell metacharacters in the path info to cgi-bin/.	Version(s):Firmware <1.0.3.26, <1.0.0.28, <1.0.0.46, <1.0.7.6, <1.0.1.14, <1.0.1.8, <1.0.4.6.	Published - December 09, 2016 CVE-2016-6277 CVSS - 9.3 Vendor's Advisory Available at: http://kb.netgear.com/000036386/CVE-2016-582384
Adobe Flash Player <=23.0.0.207, <=11.2.202.644 Remote Use-After-Free Vulnerability - CVE-2016-7881	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.	Version(s): Flash Player <=11.2.202.644, <=23.0.0.207	Published - December 13,2016 CVE-2016-7881 CVSS - 9.3 Vendor's Advisory Available at: http://www.securityfocus.com/bid/94873
Mozilla Firefox 50.0.2 Remote Code Execution due to Multiple Memory Corruption Issues	Mozilla Firefox version 50.0.2 is prone to a remote code execution vulnerability, due to multiple memory corruption issues.	Version(s): Firefox 50.0.2	Published - December 13,2016 CVE-2016-9080 CVSS - 9.3 The vendor's advisory is available at: https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/
Mozilla Firefox <50.1 and Firefox ESR <45.6 Remote Code Execution due to Multiple Memory Corruption Issues	Mozilla Firefox prior to 50.1, Firefox ESR prior to 45.6, and Thunderbird prior to 45.6 are prone to a remote code execution vulnerability, due to multiple memory corruption issues.	Version(s): Firefox <50.1, <ESR 45.6	Published -December 13,2016 CVE-2016-9893 CVSS - 9.3 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2016-95/
[MS16-144] Microsoft Internet Explorer Memory Corruption Vulnerability - CVE-2016-7279	Microsoft Internet Explorer 9, 10, and 11 do not properly access objects in memory making them prone to a remote code execution vulnerability. A remote attacker who could entice the victim to visit a maliciously crafted website could exploit this issue to execute arbitrary code in the context of the current user.	Version(s): Internet Explorer 10, 9, 11.	Published -December 13,2016 CVE-2016-7279 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms16-144
[MS16-146] Microsoft Windows Remote Code Execution in Windows Graphics - CVE-2016-7272	Windows Graphics in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 and Server 2012 R2, Windows 10, Windows 10 version 1511, Windows 10 version 1607 and Windows Server 2016 allows a remote attacker to execute arbitrary code via a crafted file.	Version(s): Windows 7, Server 2008 R2, 8, Server 2016, Vista, Server 2008, Server 2012 R2, Server 2012, 10.	Published - December 13,2016 CVE-2016-7272 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms16-146
Mozilla Firefox <50.1 Remote Code Execution due to a Buffer Overflow in SkiaGL	Mozilla Firefox prior to 50.1 is prone to a remote code execution vulnerability, due to a buffer overflow in SkiaGL.	Version(s) :Firefox <50.1	Published - December 13, 2016 CVE-2016-9894 CVSS - 9.3 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/
[MS16-154] Microsoft Windows Remote Code Execution in Adobe Flash Player - CVE-2016-7875	Adobe Flash Player versions 23.0.0.207 and earlier on Microsoft Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016 allows a remote attacker to execute arbitrary code via a crafted web site.	Version(s): Flash Player Any version.	Published - December 13, 2016 CVE-2014-7875 CVSS - 9.3 Vendor's Advisory Available : https://technet.microsoft.com/library/security/ms16-154
[cisco-sa-20161221-cco] Cisco CloudCenter Orchestrator Docker Engine <4.6.2 Remote Escalation of Privileges Vulnerability	Cisco CloudCenter Orchestrator before 4.6.2 is prone to an elevation of privileges due to misconfiguration that could allow a remote unauthenticated attacker to reach the docker engine ports from outside the CloudCenter Orchestrator system. The attacker can exploit this vulnerability to load docker containers on the affected system with higher privileges.	Version(s): CloudCenter Orchestrator <4.6.2	Published - December 21,2016 CVE-2016-9223 CVSS - 9.3 Vendor's Advisory Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161221-cco
VMWare vSphere Data Protection Remote Privilege Escalation due to Improper Handling of a Private SSH Key	VMWare vSphere Data Protection 5.5.x, 5.8.x, 6.0.x and 6.1.x allows a remote attacker to gain privileges due to improper handling of a private SSH key.	Version(s): Vsphere Data Protection(VDP) 5.5.*, 5.8.*, 6.0.*, 6.1.*.	Published - December 20, 2016 CVE-2015-7456 CVSS -10.0 Vendor's Advisory Available: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7456