PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Adobe Acrobat, Acrobat DC, Reader and Reader DC Remote Code Execution Vulnerability	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors	Version(s): Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X	Published - October 21,2016 CVE-2016-7852 CVSS - 9.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/acrobat/apsb16-33.html
Cisco ASA Remote Code Execution or DoS via a Crafted NetBIOS Packet	Buffer overflow in Cisco ASA 9.4(2) allows a remote attacker to cause a denial-of-service or execute arbitrary code via a crafted NetBIOS packet.	Version(s):Cisco ISA 3000 Industrial Security Appliance 0; Cisco Catalyst 7600 Series ASA Services Module 0; Cisco Catalyst 6500 Series ASA Services Module 0;Cisco ASA for Firepower 9300 Series 0;Cisco ASA for Firepower 4100 Series 0;Cisco ASA 5500-X Series Next-Generation Firewalls 0;Cisco ASA 5500 Series Adaptive Security Appliances 0; Cisco Asa 1000V Cloud Firewall 0;Cisco Adaptive Security Virtual Appliance (ASAv) 0; Cisco Adaptive Security Appliance Software 9.5, 9.4 , 9.3 , 9.0,9.1,8.7, 8.6, 8.5; Cisco Adaptive Security Appliance (ASA) Software 9.6, 9.2;Cisco Adaptive Security Appliance (ASA) 8.4	Published - October 19,2016 CVE-2016-6432 CVSS - 9.3 Vendor's Advisory Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-idfw
Remote Code Execution Vulnerability in GD dynamicGetbuf	A stack-buffer overflow in GD dynamicGetbuf in PHP 7.0.11 allows remote attackers to execute arbitrary code.	Version(s): PHP PHP 7.0.11 LibGD LibGD 0	Published - October 17, 2016 CVE-2016-8670 CVSS - 7.5 Vendor's Advisory Available at: http://www.securityfocus.com/bid/93594
PHP 5.0 before 5.6.27 and 7.0 before 7.0.12 Remote Code Execution due to Use-After-Free	Use-after-free in unserialize function in PHP 5.0 before 5.6.27 and 7.0 before 7.0.12 allows remote attackers to execute arbitrary code via unspecified vectors.	Version(s):PHP 5.0 before 5.6.27 and 7.0 before 7.0.12	Published - October 14,2016 SBV-64168 CVSS - 7.5 The vendor's advisory is available at: http://www.securityfocus.com/bid/93577
Adobe Flash Player <= 23.0.0.162 Remote Code Execution	A memory corruption vulnerability in Adobe Flash Player version 23.0.0.162 and earlier on Windows and OS X, Flash Player ESR version 18.0.0.375 and earlier on Windows and OS X, Flash Player version 23.0.0.162 and earlier for Google Chrome, Microsoft Edge and Internet Explorer 11, and Adobe Flash Player for Linux version 11.2.202.635 and earlier, allows remote attackers to execute arbitrary code.	Version(s): Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux	Published -October 12,,2016 CVE-2016-6984 CVSS - 9.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/flash-player/apsb16-32.html
PHP 5.0 before 5.6.27 and 7.0 before 7.0.12 Remote Code Execution via a Crafted Command	Heap buffer overflow in virtual_popen in file zend_virtual_cwd.c in PHP before 5.6.27 and 7.0 before 7.0.12 allows remote attackers to execute arbitrary code by using a very long command.	Version(s):PHP before 5.6.27 and 7.0 before 7.0.12	Published -October 14,2016 SBV-64167 CVSS - 7.5 The vendor's advisory is available at: http://www.securityfocus.com/bid/93574
Linux Kernel 3.13 through 4.5.5 Remote DoS via Crafted Packets	Linux Kernel 3.13 through 4.5.5, when GRO is enabled, allows a remote Attacker to cause a denial-of-service via crafted packets.	Version(s): Linux kernel before 4.6	Published - October 14,2016 CVE-2016-8666 CVSS -7.8 Vendor's Advisory Available at http://www.securityfocus.com/bid/93562
Microsoft Windows Remote Code Execution in Adobe Flash Player	Adobe Flash Player on Microsoft Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10, Windows 10 1511, and Windows 10 1607, is prone to a remote code execution vulnerability due to a memory corruption issue.	Version(s):Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux	Published - October 11, 2016 CVE-2016-4273 CVSS - 9.3 Vendor's Advisory Available at https://www.adobe.com/software/flash/about/
Adobe Acrobat, Acrobat DC, Reader and Reader DC Remote Code Execution Vulnerability	Memory corruption in Adobe Acrobat DC Continuous 15.017.20053 and earlier, Acrobat Reader DC Continuous 15.017.20053 and earlier, Acrobat DC Classic 15.006.30201 and earlier, Acrobat Reader DC Classic 15.006.30201 and earlier, Acrobat XI 11.0.17 and earlier and Reader XI 11.0.17 and earlier allow remote attackers to execute arbitrary code via unspecified vectors.	Version(s):Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X	Published - October 11, 2016 CVE-2016-7012 CVSS - 9.3 Vendor's Advisory Available : https://helpx.adobe.com/security/products/acrobat/apsb16-33.html
Microsoft Internet Explorer 11 Remote Code Execution in Scripting Engine	The Scripting Engine in Microsoft Internet Explorer 11, does not properly render when handling objects in memory, making it prone to a remote memory corruption vulnerability. A remote attacker who could entice the victim to visit a specially crafted website, or to open a malicious application or file, could exploit this issue to execute arbitrary code on the affected computer with the privileges of the current user.	Version(s): Microsoft Internet Explorer 11 and Microsoft Edge	Published -October 11, 2016 CVE-2016-3390 CVSS - 9.3 Vendor's Advisory Available at: https://support.microsoft.com/en-us/products/internet-explorer
Microsoft Edge Remote Code Execution in Chakra JavaScript Scripting Engine	The Chakra JavaScript Scripting Engine in Microsoft Edge does not properly render when handling objects in memory, making it prone to a remote memory corruption vulnerability. A remote attacker who could entice the victim to visit a specially crafted website, or to open a malicious application or file, could exploit this issue to execute arbitrary code on the affected computer with the privileges of the current user.	Version(s): Microsoft Internet Explorer 9 through 11 and Microsoft Edge	Published -October 11, 2016 CVE-2016-3382 CVSS - 9.3 Vendor'sAdvisoryAvailable: https://technet.microsoft.com/library/security/ms16-119
Microsoft Windows Font Library Remote Code Execution Vulnerability	Microsoft Windows Vista, Windows Server 2008 , Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10, Windows 10 1511, Windows 10 1607, Office 2007, Office 2010, Word Viewer, Skype for Business 2016, Lync 2013, Lync 2010, and Live Meeting 2007 Console, are prone to a remote code execution vulnerability due to an issue in the way the Windows font library handles certain embedded fonts. A remote attacker who could entice the victim to open a specially crafted file or to visit a specially crafted website, could exploit this issue to execute arbitrary code on the affected system.	Version(s): 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; 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	Published -October 11, 2016 CVE-2016-3396 CVSS - 9.3 Vendor's Advisory Available: https://technet.microsoft.com/library/security/ms16-120
Microsoft Multiple Office Products Remote Code Execution Vulnerability	Microsoft Office 2010 SP2, Compatibility Pack SP3, Web Apps 2010 SP2, Web Apps Server 2013 SP1 and Word 2007 SP3, 2010 SP2, 2013 SP1, 2013 SP1 RT, 2016, and Word 2011 and 2016 for Mac, and Word Viewer are prone to a remote code execution vulnerability due to improper handling in RTF files in Microsoft Office Software.	Version(s): Microsoft Word 2007 SP2, Office 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server	Published -October 11, 2016 CVE-2016-7193 CVSS - 9.3 Vendor's Advisory Available: https://technet.microsoft.com/library/security/ms16-121