Histórico de vulnerabilidades de Marzo del 2016

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Php	Use-after-free vulnerability in widsk.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triberine and wide describility call on WIL data containing a crafted var element.	31/03/2016	<u>10.0</u>	CVE-2016-3141
Googlechrome	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	29/03/2016	93	CVE-2016-3679
Cogentdatahub	Cogent DataHub before 7.3.10 allows local users to gain privileges by leveraging the user or guest role to modify a file.	29/03/2016	7.2	CVE-2016-2288
Googlechrome	The PageCaptureSaveAkMHTMLFunction=ReturnFailure function in browser/extensions/api/page_capture/page	29/03/2016	<u>93</u>	CVE-2016-1650
Googlechrome	The Program:getUniformInternal function in Program.cpp in IIbANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via cartled stader stage.	29/03/2016	<u>9.3</u>	CVE-2016-1649
Googlechrome	Use-ster-free vulnerability in the GetLoadTimes function in enderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unseecified other impact via crafted JavaScript code.	29/03/2016	<u>9.3</u>	CVE-2016-1648
Googlechrome	Use-after-free vulnerability in the RenderWidgetHostImpl=Destroy function in content/forwark/medinere/nort/neder_widget_host_inpl.c in the Navigation implementation in Google Chrome before 49.0.262.3108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	29/03/2016	<u>9.3</u>	CVE-2016-1647
Googlechrome	The Array, prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.	29/03/2016	<u>9.3</u>	CVE-2016-1646
Autodeskbackburner	Stack-based baffer overflow in manager-zee in Backburner Manager in Autodesk Backburner 2016 2016.0.0.2150 and earlier allows remote stackers to sexucit arbitrary code or cause a denial of service (desmon crash) vas carlied command. NOTE, this is only avulnerability in environments in which the administrator has not followed documentation that outlines the security risks of operating Backburrer on untruteen environs.	28/03/2016	<u>7.8</u>	CVE-2016-2344
Pcre	pcre_jit_compile_c in PCRE 8.35 does not properly use table jumps to optimize nested alternatives, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a crafted string, as demonstrated by packet encountered by Sucrical duming use of a regular arguezion in an Emerging Threats Open ruleset.	28/03/2016	7.5	CVE-2014-9769

	Semana 21/03/2016			
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Ciscoios	The Locator/ID Separation Protocol (LISP) implementation in Cisco IOS 15.1 and 15.2 and NX-OS 4.1 through 6.2 allows remote attackers to cause a denial of service (device reload) via a crafted header in a packet, aka Bug ID CSCuu64279.	25/03/2016	7.8.	CVE-2016-1351
Ciscoios	Cisco IOS 15.3 and 15.4, Cisco IOS XE 3.8 through 3.11, and Cisco Unified Communications Manager allow remote attackers to cause a denial of service (device reload) via malformed SIP messages, aka Bug ID CSCu(23293.	25/03/2016	<u>7.8</u>	CVE-2016-1350
Ciscoios	The Smart Install client implementation in Cisco IOS 12.2, 15.0, and 15.2 and IOS XE 3.2 through 3.7 allows remote attackers to cause a denial of service (device reload) via crafted image list parameters in a Smart Install packet, aka Bug ID CSCuv45410.	25/03/2016	<u>7.8</u>	CVE-2016-1349
Ciscoios	Cisco IOS 15.0 through 15.5 and IOS XE 3.3 through 3.16 allow remote attackers to cause a denial of service (device reload) via a crafted DHCPv6 Relav message, aka Bue ID CSCusS5821.	25/03/2016	7.8	CVE-2016-1348
Ciscoios	The Wide Area Application Services (WAAS) Express implementation in Cisco IOS 15.1 through 15.5 allows remote attackers to cause a denial of service (device reload) via a crafted TCP segment, aka Bug ID CSCuq59708.	24/03/2016	7.8	CVE-2016-1347
Apple-safari	WebKit in Apple IOS before 9.3, Safari before 9.1, and tvOS before 9.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	23/03/2016	<u>9.3</u>	CVE-2016-1783
Apple-safari	WebKit in Apple IOS before 9.3 and Safari before 9.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	23/03/2016	9.3	CVE-2016-1778
Apple-apple	TrueTypeScaler in Apple IOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file.	23/03/2016	<u>9.3</u>	CVE-2016-1775
Apple-safari	The Downloads feature in Apple Safari before 9.1 mishandles file expansion, which allows remote attackers to cause a denial of service via a crafted web site.	23/03/2016	<u>7.1</u>	CVE-2016-1771
Apple-safari	libxml2 in Apple IOS before 9.3, OS X before 10.11.4, Safari before 9.1, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.	23/03/2016	<u>10.0</u>	CVE-2016-1762
Applemac	libxml2 in Apple IOS before 9.3, OS X before 10.11.4, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.	23/03/2016	<u>10.0</u>	CVE-2016-1761
Applemac	The kernel in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1759
Applemac	Race condition in the kernel in Apple iOS before 9.3 and OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1757
Applemac	The kernel in Apple IOS before 9.3 and OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1756
Apple-apple	The kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than OLF-016-0174.	23/03/2016	<u>9.3</u>	CVE-2016-1755
Apple-watchos	The kernel in Apple IOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016 1755.	23/032016	9.3	CVE-2016-1754
Appleiphone	Multiple integer overflows in the kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allow attackers to execute arbitrary code in a privileged context via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1753
Apple-watchos	The kernel in Apple IOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to cause a denial of service via a crafted app.	23/03/2016	93	CVE-2016-1752
Apple-watchos	The kernel in Apple IOS before 9.3, tvOS before 9.2, and watchOS before 2.2 does not properly restrict the execute permission, which allows attackers to bypass a code-signing protection mechanism via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1751
Apple-watchos	Use-after-free vulnerability in the kernel in Apple IOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1750
Applemac	IOUSBFamily in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	23/03/2016	<u>9.3</u>	CVE-2016-1749
Applemac	IOGraphics in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1746.	23/03/2016	93	CVE-2016-1747
Applemac	IOGraphics in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1747.	23/03/2016	<u>9.3</u>	CVE-2016-1746
Applemac	The Intel driver in the Graphics Drivers subsystem in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016- 1743	23/03/2016	<u>93</u>	CVE-2016-1744
Applemac	The Intel driver in the Graphics Drivers subsystem in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-	23/03/2016	<u>9.3</u>	CVE-2016-1743
Applemac	The NVIDIA driver in the Graphics Drivers subsystem in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a scholar dependent of the graphics of the second	23/03/2016	10.0	CVE-2016-1741
Apple-watchos	priveged context or cause a demin or service (memory controportion) was a charted app. FontParser in Apple IOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to even use writerau role or cause a demin of remine (memory controlled) with a crafted BDE document	23/03/2016	<u>9.3</u>	CVE-2016-1740
Applemac	dyld in Apple OS X before 10.11.4 allows attackers to bypass a code-signing protection mechanism via a modified app.	23/03/2016	7.2	CVE-2016-1738
Applemac	Bluetooth in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory comunition) via a crafted ann a different vulnerability than CVE-2016-1725	23/03/2016	9.3	CVE-2016-1736
Applemac	Bluetooth in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruntion) via a crafted ann a different vulnerability than CVE-2016-1726.	23/03/2016	<u>9.3</u>	CVE-2016-1735
Appleiphone	AppleUSBNetworking in Apple IOS before 9.3 and OS X before 10.11.4 allows physically proximate attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted USB device.	23/03/2016	7.2	CVE-2016-1734
Applemac	AppleRAID in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory contruction) via a coaffeed ann	23/03/2016	<u>9.3</u>	CVE-2016-1733
Hpservice	HPE Service Manager (SM) 9.3x before 9.35 P4 and 9.4x before 9.41.P2 allows remote attackers to execute arbitrary commands via a crafter service in the service of the ser	22/03/2016	10.0	CVE-2016-1998
Hpoperations	HPE Operations Orchestration 10 x before 10.51 and Operations Orchestration content before 1.7.0 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library.	22/03/2016	<u>10.0</u>	CVE-2016-1997

Semana 14/03/2016				
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Hpsupport	HP Support Assistant before 8.1.52.1 allows remote attackers to bypass authentication via unspecified vectors.	19/03/2016	10.0	CVE-2016-2245
Symantecendpoint	The SysPlant-sys driver in the Application and Device Control (ADC) component in the client in Symantee Endpoint Protection (SEP) 12.1 before RUG-MP4 allows remote attackers to execute arbitrary code via a crafted HTML document, related to "RWX Permissions."	18/03/2016	<u>9.3</u>	CVE-2015-8154
Symantecendpoint	SQL injection vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RUG-MP4 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.	18/03/2016	83	CVE-2015-8153
Symantecendpoint	Cross-site request forgery (CSRF) vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RUG-MP4 allows remote authenticated users to hijack the authentication of administrators for requests that execute arbitrary code by adding lines to a lossing script.	18/03/2016	<u>8.5</u>	CVE-2015-8152
Ibmtiboli	** DISPUTED ** IBM Tiveli NetView Access Services (NVAS) allows remote authenticated users to gain privileges by entering the ADM command and modifying a "page IO" field to the EMSPG2 transaction code. NOTE: the vendor's perspective is that configuration and use of available security controls in the NVAS product millinges the reported vulnerability.	18/03/2016	<u>9.0</u>	CVE-2014-9768
Hpsystem	HPE System Management Homepage before 7.5.4 allows remote attackers to execute arbitrary code via unspecified vectors.	18/03/2016	<u>10.0</u>	CVE-2016-1995
Pcrepcre	The compile_branch function in prog_compile_in in PGRE 8.x before 8.39 and proc2_compile_in PGRE before 10.22 mixhandles patterns containing an (MACEFF) buildring in compilencies with neted patternstees, which allows remote attackers to execute arbitrary code or cause a denial of service (tatack-based builfer overflow) via a crafted regular expression, as demonstrated by a baseksrigte Roging object encountered by Incoursen, as 201CAA9342.	17/03/2016	7.5	CVE-2016-3191
Dameware	Stack-based buffer overflow in dwrcs.exe in the dwmrcs daemon in SolarWinds DameWare Mini Remote Control 12.0 allows remote attackers to execute arbitrary code via a crafted string.	17/03/2016	10.0	CVE-2016-2345
Quagga-quagga	he bgg_inli_pane_uprv4 function in bgg_mploypn.c in the VPNv4 NLRI parser in bgpd in Quagga before 1.0.20160309, when a cretain VPNv4 configuration is used, relies on a Labeled-VPN SAR Fourter-data length field during a data copy, which allows remote attackers to execute abiticry code or cause a demid of service (tack-based buffer overblow) via a crafted packet.	17/03/2016	<u>7.6</u>	CVE-2016-2342
Hpnetwork	HPE Network Automation 9.22 through 9.22.02 and 10.x before 10.00.02 allows remote attackers to execute arbitrary code or obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-1988.	14/03/2016	10.0	CVE-2016-1989
Hpnetwork	HPE Network Automation 9.22 through 9.22.02 and 10.x before 10.00.02 allows remote attackers to execute arbitrary code or	14/03/2016	10.0	CVE-2016-1988

Histórico de vulnerabilidades de Marzo del 2016

Primary Vendor Product	Semana 07/03/2016 Description	Published	CVSS Score	Source & Patch Info
Google-chrome	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google	12/02/2016		05.000.105
Cought-chronic	Clinome period +3.0.2023.67, anow remote attackers to classe a version or server (incorrect class and our or output on possibly have suspectified other impact via cardiad JPG 2000 data. WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict	15/05/2010	23	CVE-2010-1045
Googlechrome	relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.	13/03/2016	<u>9.3</u>	CVE-2016-1644
Googlechrome	The imageInputType::emsurPrimaryContent function in WebRI/Source/contPitml/Grams/ImageInputType.censurPrimaryContent function in WebRI/Source/contPitml/Grams/ImageInputType.cop in Billink, as used in Google Chrome Berror 49.0.2523, Josen net properly ministain the user agent hadwor DMD, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that levenage "type confusion." The transmission of the service of t	13/03/2016	<u>93</u>	CVE-2016-1643
Mozilla-firefox	Figure during the second of the graphice action and the second of the second action of the second action of the second of the	13/03/2016	<u>9.3</u>	CVE-2016-2799
Mozilla-firefox	Race condition in the GetStaticInstance function in the WebRTC implementation in Mozilla Firefox before 45.0 might allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via unspecified vectors.	13/03/2016	<u>9.3</u>	CVE-2016-1973
Mozilla-firefox	Integer underflow in the srtp_unprotect function in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via	13/03/2016	9.3	CVE-2016-1970
Mozillafirefox	unknown vectors. Use-after-free vulnerability in the mozilla::DataChannelConnection::Close function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code by leveraging mishandling of WebRTC data-channel	13/03/2016	10.0	CVE-2016-1962
	connections. Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 13.2 03.527 on Linux, Adobe AIR Refore 21.0.0.376, Adobe AIR SDR before 23.0.0.176, and Adobe AIR SDR & Compiler			
Adobeair sdk	Derive 112.202.577 off lows attackers to execute arbitrary code via sork benue 21.00.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-0993.	12/03/2016	<u>10.0</u>	CVE-2016-1010
Adobeflash player	Adobe Flaibh Flayer before 18.00.333 and 9.4 kmoggi 1.1. kefore 21.0.0.182 on Windows and 05 X and before 11.0.20.75 on Linux, Adobe AB More 21.00.176, Adobe AB SD & Mofere 21.0.0.176, and Adobe AB SD & & Complex Enfort 21.0.0.175, and etal.adors to execute arbitrary code or cause a detail of service (unitalized pointer dereference and memory comparison) and etal.adors 10.0000 (2000)	12/03/2016	<u>93</u>	CVE-2016-1005
Adobeflash player	Adobe Flash Player before 18.00.333 and 19.x through 21.x before 21.0.0.182 on Windows and 05 X and before 11.2.202.577 on Linux, Ababe AIR before 21.0.0.176, Adobe AIR SOB before 21.0.0.176, and Adobe AIR SOB & Compliar before 21.0.0.176 allow attackers to executive autitary code or care advised for size a density of size advised to support the size of the winderschilter that the Compliance advised for the Compliance advised for the Compliance advised and winderschilter that the Compliance advised for the Compliance advised for the Compliance advised and winderschilter that the Compliance advised for the Compliance advised for the Compliance advised advise	12/03/2016	<u>10.0</u>	CVE-2016-1002
Adobeflash player	AUE-1005. Heap-based buffer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK &	12/03/2016	10.0	CVE-2016-1001
	Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors. Use-after-free vulnerability in Adobe Flash Player before 18.00.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK &			
Adobeflash player	Complete before 21.0.0.176 Jakova sittakers to rescut a abbitrary code via unspecified vectors, a different vulnerability than CVE- 2016-0997, CVE-2016-0998, CVE-2016-0999, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0996, CVE-2016-0998, and CVE-2016-0999. Uwa sitte-free vulnerability in Adolem Flah Plager before 18.0.0.333 and 15 x through 21 x before 21.0.0.122 on Windows and OS	12/03/2016	10.0	CVE-2016-1000
Adobeflash player	X and before 11.2.20.577 on Linux, Adobe Alfk Before 21.0.21%, Adobe Alfk SDk Before 21.0.0.176, and Adobe Alfk SDk & Compler before 71.0.01% allows attactives to secure abritary code via ungeofficie vectora, adferent vulnerability than CVF- 2016-0987, CVF-2016-0988, CVF-2016-0999, CVF-2016-0991, CVF-2016-0995, CVF-2016-0995, CVF-2016-0995, CVF-2016-0997, CVF-2016-0988, and CVF-2016-0997, CVF-2016-0991, CVF-2016-0995, CVF-2016-0995, CVF-2016-0995, CVF-2016-0997, CVF-2016-0988, and CVF-2016-0997, CVF-2016-0991, CVF-2016-0995, CVF-2016-0995, CVF-2016-0997, CVF-2016-097, CVF-2016-097, CVF-2016-097, CVF-2016-097, CVF-2007, CVF-2016-097, CVF-2016-0	12/03/2016	<u>10.0</u>	CVE-2016-0999
Adobeflash player	Use-attentive vulnerability in Adobe Fisah Player before 18.0.0.333 and 19.4 through 21.4 before 21.0.0.182 on Windows and OS X and before 11.20.577 on Linux, Adobe AF Bofer 21.0.0.176, Adobe AFI SDK Edver 21.0.0.176, adobe AFI SDK & Complete before 21.0.0.176, adobes attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVF- 2016-0897, CVF-2016-0998, CVF-2016-0999, CVF-2016-0994, CVF-2016-0994, CVF-2016-0996, CVF-2016-09997, CVF-2016-0997, and CVF-2016-0900.	12/03/2016	<u>10.0</u>	CVE-2016-0998
Adobeflash player	Uue-alter-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.4 sthrough 21. before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe All Before 21.0.0.176, Adobe All'S DK before 21.0.0.176, and Adobe All'S DK & Compler before 21.0.0.176 silows statckers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE- 2016-0998, CVE-2016-0998, CVE-2016-0999, CVE-2016-0994, CVE-2016-0995, CVE-2016-0998, CVE-2016-0998, CVE-2016-0998, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0998, CVE-2016-098, CVE-2016-098, CVE-2016-098, CVE-2016-098, CVE-2016-098, CVE-2016-098, CVE-2016-098, CVE-2016-098, C	12/03/2016	<u>10.0</u>	CVE-2016-0997
Adobeflash player	Use-after-free vulnerability in the settinterval method in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.126 are Windows and GSX and before 11.2.202.577 on Linux, Adobe Alik Before 21.0.0.176, Adobe Alik SGX before 21.0.0.176, and Adobe Alik SGX & Complete before 21.0.0.176 align Adobe Alik SGX before 21.0.0.176, and Adobe Alik SGX & Complete before 21.0.0.176 align Adobe Alik SGX before addifferent vulnerability than (VC-5016/088), (VE-5016/0980, (VE-2016/0991, CVE-2016/0995, CVE-2016/095, CVE-2016/095	12/03/2016	<u>9.3</u>	CVE-2016-0996
Adobeflash player	Circle and experimentality in Addee Teals Physer before 18:00.333 and 19:x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2:20:577 on Linux, Addee AIR before 21.0.0.1%, Addee AIR SDK before 21.0.0.1%, and Addee AIR SDK & Compler before 31.2:0.1% allow attaches to securit abitizer code via unspecified weters, a different viniteriality than CVF- 2016-0931, CVF-2016-0938, CVF-2016-0930, CVF-2016-0931, CVF-2016-0934, CVF-2016-0939, CVF-2016-0930, CVF-20	12/03/2016	<u>10.0</u>	<u>CVE-2016-0995</u>
Adobeflash player	Use after free vulnerability in Adobe Flah Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.02.577 on Linux, Adobe All Before 21.0.0.178, Adobe All SOC before 21.0.0.176, and Adobe All SOC & Compler More 21.0.0173 allows attackers to execute abilitary one buy using the actional/Buhlod spondo with Caffed arguments, a different vulnerability than CVF-2016-0988, CVF-2016-0989, CVF-2016-0998, CVF-2016-0998, CVF-2016-0998, CVF-2016-0998, CVF-2016-0998, CVF-2016-0098, CVF-2016-0008, CVF-2016-	12/03/2016	<u>93</u>	<u>CVF-2016-0994</u>
Adobeflash player	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21. before 21.0.0.182 on Windows and OS X and before 11.2.702.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute abilityra code via ungerelide vectors, a different vulnerability than CVE-2016 (993)	12/03/2016	<u>10.0</u>	CVE-2016-0993
Adobeflash player	and CVE-2016-1010. Addbe Flach Hyper Hefner 18.0.0.333 and 19.x through 21.x before 21.0.0.132 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SOK before 21.0.0.176, and Adobe AIR SOK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (immony corruption) via unspecified vectors, a different whenehality Hand V-2016-0660, CVE 2016-0562, CVE 2016-0562, CVE 2016-0680, CVE 2016-0689, CVE 2016-089, CVE 2016-080, CVE 2016-080	12/03/2016	<u>10.0</u>	CVE-2016-0992
Adobeflash player	2016-1005. Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176 and Adobe AIR SDK & Complete Fedrer 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVF- 2016-0897, CVF-2016-0896, CVF-2016-0996, CVF-2016-0966, CVF-2016-096, CVF-	12/03/2016	<u>10.0</u>	CVE-2016-0991
Adobeflash player	CVE-2016/0999. and CVE-2016-1000. Use-after-free volenzability in Adobe Flash Physe before 18.0.0.333 and 19.x through 21.x before 21.0.0.126 and Modow Alm SDK & Complete Peter 21.0.0.176 and Adobe Alm Before 21.0.0.176, Adobe Alm SDK before 21.0.0.176, and Adobe Alm SDK & Complete Peter 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different Vulnerability than CVE- 2016-0987, CVE-2016988, CVE-2016-0997, CVE-2016-0997, CVE-2016-0995, CVE-2016-095, CVE-2016-095, CVE-2016-095, CVE-2016-0955, CVE-2016-095,	12/03/2016	<u>10.0</u>	CVE-2016-0990
Adobeflash player	CVE-2016-0999, and CVE-2016-1000. Adobe Flash Playte before 18.0.0.233 and 19.s through 21.s before 21.0.0.182 on Windows and GS X and before 11.2.202.577 on Linux, Adobe AN Before 21.0.0.176, Adobe AN SOK before 21.0.0.176, and Adobe AN SOK & Compiler before 21.0.0.176 allow attackers to execute abilitary code or cause a denial of survice (immemory corruption) via unspecified vectors, a different winerability hand - 202.616-696, CVE 2026 662, CVE 2026 662, CVE 2026 669, CVE 2026 6692, CVE 2026 662, CVE 2026 662, CVE 2026 662, CVE 2026 662, CVE 2026 6692, CVE 2026 662, CVE 2026 6692, CVE 2026 6620, CVE 2026 6692, CVE 2026 6692, CVE 2026 6692, CVE 2026 66	12/03/2016	<u>10.0</u>	CVE-2016-0989
Adobeflash player	2016-1005. Use-after-free valuerability in Adobe Flab Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.126 on Windows and OS and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Complete Peter 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVF- 2016-0897, CVF-2016-0996, CVF-2016-0997, CVF-2016-0996, CVF-2016-0966, CVF-2016-0966	12/03/2016	<u>10.0</u>	CVE-2016-0988
Adobeflash player	CV-2106/999, and CVE-2016-1000. Use-after-free vulnerability in Adobe Rah Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.126 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Complete Defore 21.0.0.176 allows attackers to execute arbitrary code via supposition divectors, a different vulnerability than CVE- 2016-0988, CVE-2016-0990, CVE-2016-0990, CVE-2016-0990, CVE-2016-0996, CVE-2016-0966, CVE-2016-096, CVE-2016-0966, CVE-	12/03/2016	<u>10.0</u>	CVE-2016-0987
Adobeflash player	CV-2106/999, and CVF-2016-1000. Adobe Flush Player before: ISB.0.133 and IPs through 21 a before 21.0.0.136 on Windows and OS K and before 11.2.202.577 on Linux, Adobe AR before 21.0.0.176, Adobe AR SOK before 21.0.0.176, and Adobe AR SOK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory compution) via unspecified vectors, a different windenability Hun C-2016-0690, CV-2016-0605, CVF-2016-0630, CVF-2016-0892, CVF-2016-0932, CV-2016-0932, CVF-2016-0932, CVF-2016-0932, CVF-2016-0932, CVF-2016-0932, CVF-2016-0934, CVF-2016-0934	12/03/2016	<u>10.0</u>	CVE-2016-0986
Adobeflash player	2016-1005. Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVF-2016-0993 was not set of the	12/03/2016	<u>10.0</u>	CVE-2016-0963
Adobeflash player	and CV-0019-000. Addbe Flush Payer before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and 05 X and before 11.2.202.577 on Linux, Addbe AIR before 21.0.0.176, Addbe AIR SDK before 21.0.0.176, and Addbe AIR SDK & Complex before 21.0.0.176 allow attackers to execute arbitrary code or care a denial of sare/or tempory corruption) via suspecified vectors, a different vinehability than CVE-2016-0960, CVE-2016-0966, CVE-2016-0966, CVE-2016-0990, CVE-2016-0992, CVE-2016-0920, and CVE-	12/03/2016	<u>10.0</u>	CVE-2016-0962
Adobeflash player	2016 10:00 Addbe Flush Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.152 on Windows and 05 X and before 11.2.202.577 on Linux, Adobe Flush Player before 21.0.0.176, Adobe AR SDX before 21.0.0.176, and Adobe AR SDX & Complete before 21.0.0.176 allow attackers to exercise a behavior 20.0.0.176, adobe AR SDX before 21.0.0.176, and Adobe AR SDX & Complete before 21.0.0.176 allow attackers to exercise a behavior 20.0.0.176, adobe AR SDX before 21.0.0.176, and Adobe AR SDX & Complete before 21.0.0.176 allow attackers to exercise a behavior 20.000 accurate a dehald of article (hermony corruption) tak unspectified vectors, a different undersbillty than CVF-2016-0960, CVF-2016-0986, CVF-2016-0989, CVF-2016-0989	12/03/2016	<u>10.0</u>	CVE-2016-0961
Adobeair	2017 2027 Addbe Flash Have before 18.0.0.333 and 19x through 31.x before 21.0.0.182 on Windows and 05 X and before 11.2.202.577 on Unux, Adobe AR before 21.0.0.176, Adobe AR SOK Before 21.0.0.176, and Adobe AR SOK & Complete Fadore 21.0.0.176 allow Tatalaces 10 anexists. The adobe adobe adobe of the offenement composition you suppedient vectors, 24.0.016 Patients of the adobe adobe adobe adobe adobe adobe of the offenement composition you suppedient vectors, 24.001 winnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0982, CVE-2016-0022, and CVE-	12/03/2016	<u>10.0</u>	CVE-2016-0960
Ibmtivoli	<u>cure wwo.</u> The portal client in IBM Tivoli Monitoring (ITM) 6.2.2 through FP9, 6.2.3 through FP5, and 6.3.0 through FP6 allows remote authenticated users to zain orivilezes via unspecified vectors.	11/03/2016	9.0	CVE-2015-7411
Microsoftinternet	The CAttrArray object implementation in Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and memory corruption) via a malformed Cascading Style Sheets (CSS) token sequence in conjunction with modifications to HTML elements, and "Internet Findner Memory Carruption, Universiting" a	09/03/2016	<u>9.3</u>	CVE-2015-6184
Cisco-dpc	different vulnerability than CVE-2015-6048 and CVE-2015-6049. Buffer overflow in the web server on Cisco DPC2203 and EPC2203 devices with firmware r1_customer_image allows remote	09/03/2016	10.0	CVE-2016-1327
Ciscodpq docsis	attackers to execute arbitrary code via a crafted HTTP request, aka Bug ID CSCuv05935. The administration interface on Cisco DPQ3925 devices with firmware r1 allows remote attackers to cause a denial of service Idevice restartivity as a crafted HTTP reputed, aka Bug ID CSCuv83105.	09/03/2016	7.8	CVE-2016-1326
Ciscodpc wireless	The administration interface on Cisco DPC39398 and DPC3941 devices allows remote attackers to obtain sensitive information via a crafted HTP request, als Bug ID CSCus49506.	09/03/2016	<u>7.8</u>	CVE-2016-1325
Ciscoasa	The HTTPS inspection engine in the Content Security and Control Security Services Module (CSC-SSM) 6.6 before 6.6.1164.0 for Cisco ASA 5500 devices allows remote attackers to cause a denial of service (memory consumption or device reload) via a flood	09/03/2016	7.8	CVE-2016-1312
Adaba-accebat mad	of HTTPS packets, aka Bug ID CSCue76147. Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006 30121, and Acrobat and Acrobat Reader DC Cassic before 15.006 30121, and Acrobat and Acrobat Reader DC Classic before 15.006 30121, and Acrobat	00.00		0.5 2016 2022
Adobeacrobat reader	naves - co-commuso arrive a sun au access un without a sun a sun access the sun accessing and a sun accessing and accessin	09/03/2016	<u>100</u> 7.2	CVE-2016-1008

Histórico de vulnerabilidades de Marzo del 2016

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
Adobeacrobat reader	Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1009.	09/03/2016	10.0	CVE-2016-1007
Adobedigital	Adobe Digital Editions before 4.5.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	09/03/2016	10.0	CVE-2016-0954
Microsoftsharepoint server	Microsoft Word 2007 SP3, Office 2010 SP2, Word 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 and 2013 SP1, Office Web Apps 2010 SP2, and Web Apps Server 2013 SP3 allow remote attackers to execute arbitrary code via a crafted Office document, Jab "Microsoft Office Memory Compation Viderzebility".	09/03/2016	<u>93</u>	CVE-2016-0134
Microsoftnet framework	Microsoft .NET Framework 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 mishandles signature validation for unspecified elements of XML documents, which allows remote attackers to spoof signatures via a modified document, alsa ".NET XML Validation Security Feature Bysass."	09/03/2016	10.0	CVE-2016-0132
Microsoftedge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. aka "Microsoft Edge Memory Corruption Vulnerability."	09/03/2016	7.6	CVE-2016-0130
Microsoftedge	Teto any, mail microsoft Edge allows remote stackiers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0120.	09/03/2016	7.6	CVE-2016-0129
Microsoftedge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted	09/03/2016	7.6	CVE-2016-0124
Microsoftedge	web site, and whichout cure mention controllor wither builty. Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted use bits activity "Missenfer" fragmentic fragmentic programment and the service of the service (memory corruption) via a crafted	09/03/2016	7.6	CVE-2016-0123
Microsoft-windows	web site, and "Microsoft tage Memory Corruption Vulnerability." The Adobe Tryone 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	09/03/2016	9.3	CVE-2016-0121
Microsoftwindows	execute arbitrary code via a cratted Upen type tont, aka: Upen type Font Parsing Vulnerability." The PDF library in Microsoft Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF	09/03/2016	9.3	CVE-2016-0118
Microsoftwindows	document, alsa "Windows Remote Code Execution Vuinerability." 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, alsa "Windows Remote Code Execution	09/03/2016	9.3	CVE-2016-0117
Manage and an	Vulnerability." Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted			
microsoft-reage	web site, aka "Microsoft Edge Memory Corruption Vulnerability," Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory	09/03/2016	<u>1.6</u>	CVC-2016-0116
Microsoftinternet	corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,"	09/03/2016	<u>7.6</u>	CVE-2016-0114
Microsoftinternet	corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,"	09/03/2016	7.6	CVE-2016-0113
Microsoftinternet	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,"	09/03/2016	7.6	CVE-2016-0112
Microsoftedge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability,"	09/03/2016	<u>7.6</u>	CVE-2016-0111
Microsoftedge	Microsoft Internet Explorer 10 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	09/03/2016	7.6	CVE-2016-0110
Microsoft-edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability,"	09/03/2016	7.6	CVE-2016-0109
Microsoftinternet	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruntion) via a crafted web site, aka "Internet Explorer Memory Corruntion Vulnerability."	09/03/2016	7.6	CVE-2016-0108
Microsoftinternet	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory	09/03/2016	7.6	CVE-2016-0107
Microsoftinternet	corruption via a cratted web site, asa internet explorer memory corruption vulnerability; Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory	09/03/2016	7.6	CVE-2016-0106
Microsoftedge	corruption) via a crafted web site, alsa "Internet Explorer Memory Corruption Vulnerability," Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute abitrary code or cause a denial of service Memory Corruption Vulnerability "	09/03/2016	7.6	CVE-2016-0105
Microroft-internet	Microsoft Internet Explorer 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory	00/03/301/		0.0.000
Microsoft-internet	corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory	09/03/2016	7.6	CVE-2016-0104
Microsoftinternet	corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,"	09/03/2016	7.6	CVE-2016-0103
Microsoftedge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability,"	09/03/2016	7.6	CVE-2016-0102
Microsoftwindows	Microsoft Window's Server 2008 K2 SYL, Window's 7 SYL, Window's L1, Window's Server 2012 Goid and K2, Window's K1 & J, and Window's 10 Goid and 1511 allow remote attackers to execute arbitrary code via crafted media content, aka "Window's Media Parsing Remote Code Execution Vulnerability."	09/03/2016	<u>9.3</u>	CVE-2016-0101
Microsoftwindows	wicrosort windows vista 5+2 and Server 2008 SP2 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Library Loading Input Validation Remote Code Execution Vulnerability."	09/03/2016	7.2	CVE-2016-0100
Microsoftwindows	The Secondary Logon Service in Microsoft Windows Vista 592, Windows Server 2008 592 and R2 591, Windows 7594, Windows 8.1, Windows Server 2012 Gold and R2, Windows R3.1, 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 Violence/Wint".	09/03/2016	<u>72</u>	CVE-2016-0099
Microsoft-windows	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 allow remote attackers to execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Facetion Unioneability"	09/03/2016	<u>9.3</u>	CVE-2016-0098
microsoft-windows	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 and/iration ada "Win2" Elevation of Privilese Vulnerability "	09/03/2016	7.2	CVE-2016-0096
Microsoft-windows	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 apolication, a.a. ¹ Win324; Elevation of Privileges Vulnerability. ¹	09/03/2016	7.2	CVE-2016-0095
Microsoft-windows	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 F511 allows local users to gain privileges via a crafted application, als "Win32K Leviation of Privilege Vulnerability."	09/03/2016	<u>7.2</u>	CVE-2016-0094
Microsoft-windows	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 511 allows local users to gain privileges via a crafted application, adv Win32K Vieution of Privilege Vulnerability.	09/03/2016	7.2	CVE-2016-0093
Microsoft-windows	OLE In Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows 7 Server 2012 Gold and R2, Windows R1 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, als A "Windows DLE Memory Remote Code Secucion Vulnerability".	09/03/2016	<u>93</u>	CVE-2016-0092
Microsoftwindows	Microsoft Windows Vista 9/2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 do not properly validate handles, which allows local users to gain privileges via a crafted application, aka "Windows Elevation of Privilege Vulnerability."	09/03/2016	72	CVE-2016-0087
Microsoft-office	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2016 does not properly sign an unspecified binary file, which allows local users to gain privileges via a Trojan horse file with a crafted signature, aka "Microsoft Office Security Feature Bypass Vulnerability."	09/03/2016	<u>72</u>	CVE-2016-0057
Microsoftinfopath	Microsoft infoPath 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/03/2016	9.3	CVE-2016-0021