Histórico de vulnerabilidades de Marzo del 2016

Semana 28/03/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Php	Use-after-free vulnerability in wddx.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 triggering a wddx_deserialize call on XML data containing a crafted var element.	31/03/2016	10.0	CVE-2016-3141
Google--chrome	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	9.3	CVE-2016-3679
Cogent--datahub	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
Google--chrome	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.	29/03/2016	9.3	CVE-2016-1650
Google--chrome	The Program::getUniformInternal function in Program.cpp in libANGLE, 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 crafted shader stages.	29/03/2016	9.3	CVE-2016-1649
Google--chrome	Use-after-free vulnerability in the GetLoadTimes function in renderer/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 unspecified other impact via crafted JavaScript code.	29/03/2016	9.3	CVE-2016-1648
Google--chrome	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	29/03/2016	9.3	CVE-2016-1647
Google--chrome	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	9.3	CVE-2016-1646
Autodesk--backburner	Stack-based buffer overflow in manager.exe in Backburner Manager in Autodesk Backburner 2016 2016.0.0.2150 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted command. NOTE: this is only a vulnerability in environments in which the administrator has not followed documentation that outlines the security risks of operating Backburner on untrusted networks.	28/03/2016	7.8	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 packets encountered by Suricata during use of a regular expression 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
Cisco--ios	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
Cisco--ios	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 CSCuj23293.	25/03/2016	7.8	CVE-2016-1350
Cisco--ios	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	7.8	CVE-2016-1349
Cisco--ios	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 Relay message, aka Bug ID CSCus59821.	25/03/2016	7.8	CVE-2016-1348
Cisco--ios	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	9.3	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	9.3	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	7.1	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	10.0	CVE-2016-1762
Apple--mac	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	10.0	CVE-2016-1761
Apple--mac	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	9.3	CVE-2016-1759
Apple--mac	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	9.3	CVE-2016-1757
Apple--mac	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	9.3	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 CVE-2016-1754.	23/03/2016	9.3	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
Apple--iphone	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	9.3	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	9.3	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	9.3	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	9.3	CVE-2016-1750
Apple--mac	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	9.3	CVE-2016-1749
Apple--mac	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	9.3	CVE-2016-1747
Apple--mac	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	9.3	CVE-2016-1746
Apple--mac	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	9.3	CVE-2016-1744
Apple--mac	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-2016-1744.	23/03/2016	9.3	CVE-2016-1743
Apple--mac	The NVIDIA 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.	23/03/2016	10.0	CVE-2016-1741
Apple-watchos	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 execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document.	23/03/2016	9.3	CVE-2016-1740
Apple--mac	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
Apple--mac	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 corruption) via a crafted app, a different vulnerability than CVE-2016-1735.	23/03/2016	9.3	CVE-2016-1736
Apple--mac	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 corruption) via a crafted app, a different vulnerability than CVE-2016-1736.	23/03/2016	9.3	CVE-2016-1735
Apple--iphone	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
Apple--mac	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 corruption) via a crafted app.	23/03/2016	9.3	CVE-2016-1733
Hp--service	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 crafted serialized Java object, related to the Apache Commons Collections library.	22/03/2016	10.0	CVE-2016-1998
Hp--operations	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	10.0	CVE-2016-1997

Semana 14/03/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hp--support	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
Symantec--endpoint	The SysPlant.sys driver in the Application and Device Control (ADC) component in the client in Symantec Endpoint Protection (SEP) 12.1 before RU6-MP4 allows remote attackers to execute arbitrary code via a crafted HTML document, related to "RWX Permissions."	18/03/2016	9.3	CVE-2015-8154
Symantec--endpoint	SQL injection vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RU6-MP4 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.	18/03/2016	8.3	CVE-2015-8153
Symantec--endpoint	Cross-site request forgery (CSRF) vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RU6-MP4 allows remote authenticated users to hijack the authentication of administrators for requests that execute arbitrary code by adding lines to a logging script.	18/03/2016	8.5	CVE-2015-8152
Ibm--tivoli	** DISPUTED ** IBM Tivoli NetView Access Services (NVAS) allows remote authenticated users to gain privileges by entering the ADM command and modifying a "page ID" field to the EMSPG2 transaction code. NOTE: the vendor's perspective is that configuration and use of available security controls in the NVAS product mitigates the reported vulnerability.	18/03/2016	9.0	CVE-2014-9768
Hp--system	HPE System Management Homepage before 7.5.4 allows remote attackers to execute arbitrary code via unspecified vectors.	18/03/2016	10.0	CVE-2016-1995
Pcre--pcre	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39 and pcre2_compile.c in PCRE2 before 10.22 mishandles patterns containing an (*ACCEPT) substring in conjunction with nested parentheses, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, aka ZDI-CAN-3542.	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 bgp_nlri_parse_vpnv4 function in bgp_mplsvpn.c in the VPNv4 NLRI parser in bgpd in Quagga before 1.0.20160309, when a certain VPNv4 configuration is used, relies on a Labeled-VPN SAFI routes-data length field during a data copy, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted packet.	17/03/2016	7.6	CVE-2016-2342
Hp--network	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
Hp--network	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-2016-1989.	14/03/2016	10.0	CVE-2016-1988

Histórico de vulnerabilidades de Marzo del 2016

Semana 07/03/2016

Primary Vendor -- Product	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 Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.	13/03/2016	9.3	CVE-2016-1645
Google--chrome	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict 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	9.3	CVE-2016-1644
Google--chrome	The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."	13/03/2016	9.3	CVE-2016-1643
Mozilla--firefox	Heap-based buffer overflow in the graphite2::Slot::setAttr function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font.	13/03/2016	9.3	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	9.3	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 unknown vectors.	13/03/2016	9.3	CVE-2016-1970
Mozilla--firefox	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 connections.	13/03/2016	10.0	CVE-2016-1962
Adobe--air sdk	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 CVE-2016-0963 and CVE-2016-0993.	12/03/2016	10.0	CVE-2016-1010
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1002.	12/03/2016	9.3	CVE-2016-1005
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-1002
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors.	12/03/2016	10.0	CVE-2016-1001
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-0999.	12/03/2016	10.0	CVE-2016-1000
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0999
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0998
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0997
Adobe--flash player	Use-after-free vulnerability in the setInterval method 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 crafted arguments, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	9.3	CVE-2016-0996
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0995
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code by using the actionCallMethod opcode with crafted arguments, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	9.3	CVE-2016-0994
Adobe--flash player	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 CVE-2016-0963 and CVE-2016-1010.	12/03/2016	10.0	CVE-2016-0993
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0992
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0991
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0990
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0989
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0988
Adobe--flash player	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 & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.	12/03/2016	10.0	CVE-2016-0987
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0986
Adobe--flash player	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 CVE-2016-0993 and CVE-2016-1010.	12/03/2016	10.0	CVE-2016-0963
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0962
Adobe--flash player	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0961
Adobe--air	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 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.	12/03/2016	10.0	CVE-2016-0960
ibm--tivoli	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 gain privileges via unspecified vectors.	11/03/2016	9.0	CVE-2015-7411
Microsoft--internet	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, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6048 and CVE-2015-6049.	09/03/2016	9.3	CVE-2015-6184
Cisco--dpc	Buffer overflow in the web server on Cisco DPC2203 and EPC2203 devices with firmware r1_customer_image allows remote attackers to execute arbitrary code via a crafted HTTP request, aka Bug ID CSCuv05935.	09/03/2016	10.0	CVE-2016-1327
Cisco--dpq docsis	The administration interface on Cisco DPQ3925 devices with firmware r1 allows remote attackers to cause a denial of service (device restart) via a crafted HTTP request, aka Bug ID CSCup48105.	09/03/2016	7.8	CVE-2016-1326
Cisco--dpc wireless	The administration interface on Cisco DPC3939B and DPC3941 devices allows remote attackers to obtain sensitive information via a crafted HTTP request, aka Bug ID CSCus49506.	09/03/2016	7.8	CVE-2016-1325
Cisco--asa	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 of HTTPS packets, aka Bug ID CSCue76147.	09/03/2016	7.8	CVE-2016-1312
Adobe--acrobat 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-2016-1007.	09/03/2016	10.0	CVE-2016-1009
Adobe--acrobat reader	Untrusted search path vulnerability in 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 allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	09/03/2016	7.2	CVE-2016-1008

Histórico de vulnerabilidades de Marzo del 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--acrobat 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
Adobe--digital	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
Microsoft--sharepoint 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 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/03/2016	9.3	CVE-2016-0134
Microsoft--net 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, aka ".NET XML Validation Security Feature Bypass."	09/03/2016	10.0	CVE-2016-0132
Microsoft--edge	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
Microsoft--edge	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," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0130.	09/03/2016	7.6	CVE-2016-0129
Microsoft--edge	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-2016-0124
Microsoft--edge	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-2016-0123
Microsoft--windows	The Adobe Type 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 execute arbitrary code via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability."	09/03/2016	9.3	CVE-2016-0121
Microsoft--windows	The PDF library in Microsoft Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows Remote Code Execution Vulnerability."	09/03/2016	9.3	CVE-2016-0118
Microsoft--windows	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, aka "Windows Remote Code Execution Vulnerability."	09/03/2016	9.3	CVE-2016-0117
Microsoft--edge	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-2016-0116
Microsoft--internet	Microsoft Internet Explorer 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-2016-0114
Microsoft--internet	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-2016-0113
Microsoft--internet	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
Microsoft--edge	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	7.6	CVE-2016-0111
Microsoft--edge	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
Microsoft--internet	Microsoft Internet Explorer 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-2016-0108
Microsoft--internet	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-2016-0107
Microsoft--internet	Microsoft Internet Explorer 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-2016-0106
Microsoft--edge	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	7.6	CVE-2016-0105
Microsoft--internet	Microsoft Internet Explorer 10 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-2016-0104
Microsoft--internet	Microsoft Internet Explorer 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-2016-0103
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-2016-0102
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 Gold and 1511 allow remote attackers to execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability."	09/03/2016	9.3	CVE-2016-0101
Microsoft--windows	Microsoft Windows Vista SP2 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
Microsoft--windows	The Secondary Logon Service 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 does not properly process request handles, which allows local users to gain privileges via a crafted application, aka "Secondary Logon Elevation of Privilege Vulnerability."	09/03/2016	7.2	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 Execution Vulnerability."	09/03/2016	9.3	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 application, aka "Win32k Elevation of Privilege 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 application, aka "Win32k Elevation of Privilege Vulnerability,"	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 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability,"	09/03/2016	7.2	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 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation 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 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 file, aka "Windows OLE Memory Remote Code Execution Vulnerability."	09/03/2016	9.3	CVE-2016-0092
Microsoft--windows	Microsoft Windows Vista SP2, 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	7.2	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	7.2	CVE-2016-0057
Microsoft--infopath	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