Histórico de vulnerabilidades de Febreiro do 2016

Semana 29/02/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--chrome	Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	05/03/2016	10.0	CVE-2016-1633
Google--chrome	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action.	05/03/2016	9.3	CVE-2016-1634
Google--chrome	extensions/renderer/render_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.	05/03/2016	10.0	CVE-2016-1635
Google--chrome	The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource.	05/03/2016	7.5	CVE-2016-1636
Google--chrome	Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer.	05/03/2016	10.0	CVE-2016-1639
Google--chrome	Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.	05/03/2016	9.3	CVE-2016-1641
Google--chrome	Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	05/03/2016	10.0	CVE-2016-1642
Google--chrome	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	05/03/2016	10.0	CVE-2016-2843
Google--chrome	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.	05/03/2016	9.3	CVE-2016-2844
Adobe--air sdk	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data.	04/03/2016	9.3	CVE-2015-8652
Adobe--air sdk	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data.	04/03/2016	9.3	CVE-2015-8653
Adobe--air sdk	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data.	04/03/2016	9.3	CVE-2015-8654
Adobe--air sdk	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data	04/03/2016	9.3	CVE-2015-8655
Openssl--openssl	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.	03/03/2016	10.0	CVE-2016-0705
Openssl--openssl	Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.	03/03/2016	7.8	CVE-2016-0798
Openssl--openssl	The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data.	03/03/2016	10.0	CVE-2016-0799
Openssl--openssl	The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data.	03/03/2016	10.0	CVE-2016-2842
Schneider electric--struxureware building operations automation server	Schneider Electric Struxureware Building Operations Automation Server AS 1.7 and earlier and AS-P 1.7 and earlier allows remote authenticated administrators to execute arbitrary OS commands by defeating an msh (aka Minimal Shell) protection mechanism.	02/03/2016	9.0	CVE-2016-2278
IBM--tivoli storage manager	Stack-based buffer overflow in IBM Tivoli Storage Manager FastBack 5.5 and 6.1.x through 6.1.11.1 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	29/02/2016	10.0	CVE-2016-0216
IBM--tivoli storage manager	Stack-based buffer overflow in IBM Tivoli Storage Manager FastBack 5.5 and 6.1.x through 6.1.11.1 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	29/02/2016	10.0	CVE-2016-0213
IBM--tivoli storage manager	Stack-based buffer overflow in IBM Tivoli Storage Manager FastBack 5.5 and 6.1.x through 6.1.11.1 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	29/02/2016	10.0	CVE-2016-0212

Semana 22/02/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wireshark--wireshark	Untrusted search path vulnerability in the WiresharkApplication class in ui/qt/wireshark_application.cpp in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 on Windows allows local users to gain privileges via a Trojan horse riched20.dll.dll file in the current working directory, related to use of QLibrary.	27/02/2016	7.2	CVE-2016-2521
Inds--iartist	QNAP iArtist Lite before 1.4.54, as distributed with QNAP Signage Station before 2.0.1, allows remote authenticated users to gain privileges by registering an executable file, and then waiting for this file to be run in a privileged context after a reboot.	27/02/2016	8.5	CVE-2015-7262
Qnap--signage	The FTP service in QNAP iArtist Lite before 1.4.54, as distributed with QNAP Signage Station before 2.0.1, has hardcoded credentials, which makes it easier for remote attackers to obtain access via a session on TCP port 21.	27/02/2016	10.0	CVE-2015-7261
Qnap--signage	Unrestricted file upload vulnerability in QNAP Signage Station before 2.0.1 allows remote authenticated users to execute arbitrary code by uploading an executable file, and then accessing this file via an unspecified URL.	27/02/2016	9.0	CVE-2015-6022
Flexerasoftware--flexnet publisher	Multiple buffer overflows in (1) lmgrd and (2) Vendor Daemon in Flexera FlexNet Publisher before 11.13.1.2 Security Update 1 allow remote attackers to execute arbitrary code via a crafted packet with opcode (a) 0x107 or (b) 0x10a.	23/02/2016	10.0	CVE-2015-8277
Nettle--project nettle	The ecc_256_modq function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors.	23/02/2016	7.5	CVE-2015-8805

Semana 15/02/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--chrome	Google Chrome before 48.0.2564.116 allows remote attackers to bypass the Blink Same Origin Policy and a sandbox protection mechanism via unspecified vectors.	21/02/2016	10.0	CVE-2016-1629
Cuore--ec-cube	SQL injection vulnerability in the Help plug-in 1.3.5 and earlier in Cuore EC-CUBE allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	19/02/2016	7.5	CVE-2016-1154
Libreoffice--libreoffice	The lwp filter in LibreOffice before 5.0.4 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted LotusWordPro (lwp) document.	18/02/2016	9.3	CVE-2016-0794
Libreoffice--libreoffice	LibreOffice before 5.0.5 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted LwpTocSuperLayout record in a LotusWordPro (lwp) document.	18/02/2016	9.3	CVE-2016-0795
Microsoft--internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0069.	18/02/2016	9.3	CVE-2016-0068
Microsoft--internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0068.	18/02/2016	9.3	CVE-2016-0069
Sap--netweaver	SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2101079.	16/02/2016	7.5	CVE-2016-2386
Sap--netweaver	SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2101079.	16/02/2016	7.5	CVE-2016-2386
Sap--netweaver	SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2101079.	16/02/2016	7.5	CVE-2016-2386

Semana 08/02/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tollgrade--smartgrid_lighthouse_sensor_management_system	Cross-site request forgery (CSRF) vulnerability in Tollgrade SmartGrid LightHouse Sensor Management System (SMS) Software EMS before 5.1, and 4.1.0 Build 16, allows remote attackers to hijack the authentication of arbitrary users.	12/02/2016	7.5	CVE-2016-0863
tollgrade--smartgrid_lighthouse_sensor_management_system	Tollgrade SmartGrid LightHouse Sensor Management System (SMS) Software EMS before 5.1, and 4.1.0 Build 16, allows remote authenticated users to change arbitrary passwords via unspecified vectors.	12/02/2016	9.0	CVE-2016-0865
microsoft--word	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 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0052.	10/02/2016	9.3	CVE-2016-0022
microsoft--word	The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote authenticated users to execute arbitrary code via crafted data, aka "Remote Desktop Protocol (RDP) Elevation of Privilege Vulnerability."	10/02/2016	7.2	CVE-2016-0036
microsoft--windows	Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Memory Corruption Vulnerability."	10/02/2016	9.3	CVE-2016-0038
microsoft--windows	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka "Windows Elevation of Privilege Vulnerability."	10/02/2016	7.2	CVE-2016-0040
microsoft--windows	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 and 1511, and Internet Explorer 10 and 11 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."	10/02/2016	7.2	CVE-2016-0041
microsoft--windows	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 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "Windows DLL Loading Remote Code Execution Vulnerability."	10/02/2016	7.2	CVE-2016-0042
microsoft--windows	Windows Reader in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted Reader file, aka "Microsoft Windows Reader Vulnerability."	10/02/2016	9.3	CVE-2016-0046
microsoft--windows	The kernel-mode drivers 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 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	10/02/2016	7.2	CVE-2016-0048
microsoft--windows	The WebDAV client 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 "WebDAV Elevation of Privilege Vulnerability."	10/02/2016	7.2	CVE-2016-0051
microsoft--office	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 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0022.	10/02/2016	9.3	CVE-2016-0052

Histórico de vulnerabilidades de Febreiro do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft--office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps Server 2013 SP1, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/02/2016	9.3	CVE-2016-0053
microsoft--office	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 SP1, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/02/2016	9.3	CVE-2016-0054
microsoft--office	Microsoft Office 2007 SP3 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/02/2016	9.3	CVE-2016-0055
microsoft--office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/02/2016	9.3	CVE-2016-0056
microsoft--windows	Buffer overflow in the PDF Library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 allows remote attackers to execute arbitrary code via a crafted PDF document that triggers API calls, aka "Microsoft PDF Library Buffer Overflow Vulnerability."	10/02/2016	9.3	CVE-2016-0058
microsoft--internet_explorer	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," a different vulnerability than CVE-2016-0061, CVE-2016-0063, CVE-2016-0067, and CVE-2016-0072.	10/02/2016	9.3	CVE-2016-0060
microsoft--internet_explorer	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," a different vulnerability than CVE-2016-0060, CVE-2016-0063, CVE-2016-0067, and CVE-2016-0072.	10/02/2016	9.3	CVE-2016-0061
microsoft--internet_explorer	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."	10/02/2016	9.3	CVE-2016-0062
microsoft--internet_explorer	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," a different vulnerability than CVE-2016-0060, CVE-2016-0061, CVE-2016-0067, and CVE-2016-0072.	10/02/2016	9.3	CVE-2016-0063
microsoft--internet_explorer	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."	10/02/2016	9.3	CVE-2016-0064
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0965
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0966
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0967
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0968
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0969
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0970
adobe--flash_player	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors.	10/02/2016	10.0	CVE-2016-0971
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0972
adobe--flash_player	Use-after-free vulnerability in the URLRequest object implementation in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via a URLLoader.load call, a different vulnerability than CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.	10/02/2016	9.3	CVE-2016-0973
adobe--flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.	10/02/2016	10.0	CVE-2016-0974
adobe--flash_player	Use-after-free vulnerability in the instanceof function in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code by leveraging improper reference handling, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.	10/02/2016	9.3	CVE-2016-0975
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0976
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0977
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0978
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0980, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0979
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0981.	10/02/2016	10.0	CVE-2016-0980
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0980.	10/02/2016	10.0	CVE-2016-0981
adobe--flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0983, and CVE-2016-0984.	10/02/2016	10.0	CVE-2016-0982
adobe--flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0984.	10/02/2016	10.0	CVE-2016-0983
adobe--flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0983.	10/02/2016	10.0	CVE-2016-0984
adobe--flash_player	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."	10/02/2016	9.3	CVE-2016-0985
siemens--simatic_s7-1500_cpu_firmware	Siemens SIMATIC S7-1500 CPU devices before 1.8.3 allow remote attackers to cause a denial of service (STOP mode transition) via crafted packets on TCP port 102.	08/02/2016	7.8	CVE-2016-2200
atlassian--bamboo	The Ignite Realtime Smack XMPP API, as used in Atlassian Bamboo before 5.9.9 and 5.10.x before 5.10.0, allows remote configured XMPP servers to execute arbitrary Java code via serialized data in an XMPP message.	08/02/2016	7.5	CVE-2014-9757
atlassian--bamboo	An unspecified resource in Atlassian Bamboo before 5.9.9 and 5.10.x before 5.10.0 allows remote attackers to execute arbitrary Java code via serialized data to the JMS port.	08/02/2016	7.5	CVE-2015-8360

Semana 01/02/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sauter--moduweb_vision	Sauter EY-WSS05F0x0 moduWeb Vision before 1.6.0 sends cleartext credentials, which allows remote attackers to obtain sensitive information by sniffing the network.	06/02/2016	9.3	CVE-2015-7914
google--android	The Broadcom Wi-Fi driver in the kernel in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49G, and 6.x before 2016-02-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted wireless control message packets, aka internal bug 25662029.	06/02/2016	8.3	CVE-2016-0801
google--android	The Broadcom Wi-Fi driver in the kernel in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49G, and 6.x before 2016-02-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted wireless control message packets, aka internal bug 25306181.	06/02/2016	8.3	CVE-2016-0802
aups_snmp_web_adapter_firmware	General Electric (GE) Industrial Solutions UPS SNMP/Web Adapter devices with firmware before 4.8 allow remote authenticated users to execute arbitrary commands via unspecified vectors.	05/02/2016	9.0	CVE-2016-0861
radicale--radicale	The multifilesystem storage backend in Radicale before 1.1 allows remote attackers to read or write to arbitrary files via a crafted component name.	03/02/2016	7.5	CVE-2015-8747
radicale--radicale	The filesystem storage backend in Radicale before 1.1 on Windows allows remote attackers to read or write to arbitrary files via a crafted path, as demonstrated by /c:/file/ignore.	03/02/2016	7.5	CVE-2016-1505
apple -- mac_os_x	AppleGraphicsPowerManagement in Apple OS X before 10.11.3 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1716
apple -- apple_tv	The Disk Images component in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1717
apple -- apple_tv	The IOHIDFamily API in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1719
apple -- apple_tv	IOKit in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1720
apple -- iphone_os	The kernel in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1721
apple -- apple_tv	syslog in Apple iOS before 9.2.1, OS X before 10.11.3, and tvOS before 9.1.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	01/02/2016	7.2	CVE-2016-1722
apple--safari	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1725 and CVE-2016-1726.	01/02/2016	9.3	CVE-2016-1723
apple--safari	WebKit, as used in Apple iOS before 9.2.1, Safari before 9.0.3, and tvOS before 9.1.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1727.	01/02/2016	9.3	CVE-2016-1724
apple--safari	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1723 and CVE-2016-1726.	01/02/2016	9.3	CVE-2016-1725
apple--safari	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1723 and CVE-2016-1725.	01/02/2016	9.3	CVE-2016-1726
apple--safari	WebKit, as used in Apple iOS before 9.2.1, Safari before 9.0.3, and tvOS before 9.1.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1724.	01/02/2016	9.3	CVE-2016-1727
apple -- mac_os_x	Untrusted search path vulnerability in OSA Scripts in Apple OS X before 10.11.3 allows attackers to load arbitrary script libraries via a quarantined application.	01/02/2016	7.5	CVE-2016-1729