# Histórico de vulnerabilidades de Maio do 2016

## Semana 30/05/2016

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Imagemagick | The DrawImage function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 makes an incorrect function call in attempting to locate the next token, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. | 04/06/2016 | 7.5 | CVE-2016-4564 |
| Cisco--ip | CISCO IP 8800 phones with software 11.0.1 and earlier allow local users to gain privileges for OS command execution via crafted CLI commands, aka Bug ID CSCuz03005. | 04/06/2016 | 7.2 | CVE-2016-1403 |
| Cisco--prime | Cisco Prime Network Analysis Module (NAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) and Prime Virtual Network Analysis Module (vNAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) allow local users to obtain root access via crafted CLI input, aka Bug ID CSCuy21892. | 03/06/2016 | 7.2 | CVE-2016-1390 |
| Lenovo--accelerator | UpdateAgent in Lenovo Accelerator Application allows man-in-the-middle attackers to execute arbitrary code by spoofing an update response from susapi.lenovomm.com. | 03/06/2016 | 9.3 | CVE-2016-3944 |
| Fedoraproject | The create_script function in the lxc_container module in Ansible before 1.9.6-1 and 2.x before 2.0.2.0 allows local users to write to arbitrary files or gain privileges via a symlink attack on (1) /opt/.lxc-attach-script, (2) the archived container in the archive_path directory, or the (3) lxc-attach-script.log or (4) lxc-attach-script.err files in the temporary directory. | 03/06/2016 | 7.2 | CVE-2016-3096 |
| Cisco-network | Cisco Prime Network Analysis Module (NAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) and Prime Virtual Network Analysis Module (vNAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) allow remote attackers to execute arbitrary OS commands via a crafted HTTP request, aka Bug ID CSCuy21882. | 02/06/2016 | 7.5 | CVE-2016-1388 |
| Apache--activemq | The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request. | 01/06/2016 | 7.5 | CVE-2016-3088 |
| Apache--pdfbox | Apache PDFBox before 1.8.12 and 2.x before 2.0.1 does not properly initialize the XML parsers, which allows context-dependent attackers to conduct XML External Entity (XXE) attacks via a crafted PDF. | 01/06/2016 | 7.5 | CVE-2016-2175 |
| Sixnet--bt | Sixnet BT-5xxx and BT-6xxx M2M devices before 3.8.21 and 3.9.x before 3.9.8 have hardcoded credentials, which allows remote attackers to obtain access via unspecified vectors. | 30/05/2016 | 10.0 | CVE-2016-4521 |
| Resource--data | Resource Data Management (RDM) Intuitive 650 TDB Controller devices before 2.1.24 allow remote authenticated users to modify arbitrary passwords via unspecified vectors. | 30/05/2016 | 9.0 | CVE-2016-4505 |
| Moxa-edr | Moxa Secure Router EDR-G903 devices before 3.4.12 do not delete copies of configuration and log files after completing the import function, which allows remote attackers to obtain sensitive information by requesting these files at an unspecified URL. | 30/05/2016 | 7.8 | CVE-2016-0879 |
| Moxa-edr | Moxa Secure Router EDR-G903 devices before 3.4.12 allow remote attackers to cause a denial of service (cold start) by sending two crafted ping requests. | 30/05/2016 | 7.8 | CVE-2016-0878 |
| Moxa-edr | Memory leak on Moxa Secure Router EDR-G903 devices before 3.4.12 allows remote attackers to cause a denial of service (memory consumption) by executing the ping function. | 30/05/2016 | 7.8 | CVE-2016-0877 |
| Microsoft--windows | Untrusted search path vulnerability in the add-in installer in Adobe Connect before 9.5.3 on Windows allows local users to gain privileges via unspecified vectors. | 29/05/2016 | 7.2 | CVE-2016-4118 |
| Hp--release | The server in HP Release Control 9.13, 9.20, and 9.21 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. | 29/05/2016 | 10.0 | CVE-2016-1999 |

## Semana 23/05/2016

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Huawei--mate | Buffer overflow in the Wi-Fi driver in Huawei Mate 8 NXT-AL before NXT-AL10C00B182, NXT-CL before NXT-CL00C92B182, NXT-DL before NXT-DL00C17B182, and NXT-TL before NXT-TL00C01B182 allows attackers to cause a denial of service (crash) or possibly gain privileges via a crafted application, aka HWPSIRT-2016-03021. | 26/05/2016 | 9.3 | CVE-2016-3681 |
| Huawei--mate | Buffer overflow in the Wi-Fi driver in Huawei Mate 8 NXT-AL before NXT-AL10C00B182, NXT-CL before NXT-CL00C92B182, NXT-DL before NXT-DL00C17B182, and NXT-TL before NXT-TL00C01B182 allows attackers to cause a denial of service (crash) or possibly gain privileges via a crafted application, aka HWPSIRT-2016-03020. | 26/05/2016 | 9.3 | CVE-2016-3680 |
| Pulsesecure--pulse | Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r3, 8.0 before 8.0r11, and 7.4 before 7.4r13.4 allow remote attackers to cause a denial of service (CPU consumption) via unspecified vectors. | 26/05/2016 | 7.8 | CVE-2016-4786 |
| Fedora--project | The read_binary function in buffer.c in pgpdump before 0.30 allows context-dependent attackers to cause a denial of service (infinite loop and CPU consumption) via crafted input, as demonstrated by the \xa3\x03 string. | 26/05/2016 | 7.8 | CVE-2016-4021 |
| Canonical--ubuntu | Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow. | 26/05/2016 | 7.5 | CVE-2016-0718 |
| Freebsd | Integer signedness error in the sockargs function in sys/kern/uipc_syscalls.c in FreeBSD 10.1 before p34, 10.2 before p17, and 10.3 before p3 allows local users to cause a denial of service (memory overwrite and kernel panic) or gain privileges via a negative buflen argument, which triggers a heap-based buffer overflow. | 25/05/2016 | 7.2 | CVE-2016-1887 |
| Freebsd | Integer signedness error in the genkbd_commonioctl function in sys/dev/kbd/kbd.c in FreeBSD 9.3 before p42, 10.1 before p34, 10.2 before p17, and 10.3 before p3 allows local users to obtain sensitive information from kernel memory, cause a denial of service (memory overwrite and kernel crash), or gain privileges via a negative value in the flen structure member in the arg argument in a SETFKEY ioctl call, which triggers a "two way heap and stack overflow." | 25/05/2016 | 7.2 | CVE-2016-1886 |
| Cisco--web | Memory leak in Cisco AsyncOS through 8.8 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via an unspecified HTTP status code, aka Bug ID CSCur28305. | 24/05/2016 | 7.8 | CVE-2016-1383 |
| Cisco--web | Cisco AsyncOS before 8.5.3-069 and 8.6 through 8.8 on Web Security Appliance (WSA) devices mishandles memory allocation for HTTP requests, which allows remote attackers to cause a denial of service (proxy-process reload) via a crafted request, aka Bug ID CSCuu02529. | 24/05/2016 | 7.8 | CVE-2016-1382 |
| Cisco--web | Memory leak in Cisco AsyncOS 8.5 through 9.0 before 9.0.1-162 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via an HTTP file-range request for cached content, aka Bug ID CSCuw97270. | 24/05/2016 | 7.8 | CVE-2016-1381 |
| Cisco--web | Cisco AsyncOS 8.0 before 8.0.6-119 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (proxy-process hang) via a crafted HTTP POST request, aka Bug ID CSCuo12171. | 24/05/2016 | 7.8 | CVE-2016-1380 |
| Google--android | Lenovo SHAREit before 3.5.98_ww on Android before 4.2 allows remote attackers to have unspecified impact via a crafted intent: URL, aka an "intent scheme URL attack." | 23/05/2016 | 9.3 | CVE-2016-4782 |
| Golang--go | Untrusted search path vulnerability in Go before 1.5.4 and 1.6.x before 1.6.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function. | 23/05/2016 | 7.2 | CVE-2016-3958 |
| Huawei--mobile | The Huawei Mobile Broadband HL Service 22.001.25.00.03 and earlier uses a weak ACL for the MobileBrServ program data directory, which allows local users to gain SYSTEM privileges by modifying VERSION.dll. | 23/05/2016 | 7.2 | CVE-2016-2855 |
| Linux | The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation. | 23/05/2016 | 7.2 | CVE-2016-4951 |
| Linux | The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem. | 23/05/2016 | 7.2 | CVE-2016-4913 |
| Linux | Use-after-free vulnerability in drivers/net/ppp/ppp_generic.c in the Linux kernel before 4.5.2 allows local users to cause a denial of service (memory corruption and system crash, or spinlock) or possibly have unspecified other impact by removing a network namespace, related to the ppp_register_net_channel and ppp_unregister_channel functions. | 23/05/2016 | 7.2 | CVE-2016-4805 |
| Linux | Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denial of service (BUG) or possibly have unspecified other impact via crafted use of the mmap and bpf system calls. | 23/05/2016 | 7.2 | CVE-2016-4794 |
| Huawei--mobile | Buffer overflow in the Application Specific Packet Filtering (ASPF) functionality in the Huawei IPS Module, NGFW Module, NIP6300, NIP6600, Secospace USG6300, USG6500, USG6600, USG9500, and AntiDDoS8000 devices with software before V500R001C20SPC100 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted packet, related to "illegitimate parameters." | 23/05/2016 | 7.5 | CVE-2016-4576 |
| Linux | drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call. | 23/05/2016 | 7.2 | CVE-2016-4568 |
| Linux | The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface. | 23/05/2016 | 7.2 | CVE-2016-4565 |
| Linux | The replace_map_fd_with_map_ptr function in kernel/bpf/verifier.c in the Linux kernel before 4.5.5 does not properly maintain an fd data structure, which allows local users to gain privileges or cause a denial of service (use-after-free) via crafted BPF instructions that reference an incorrect file descriptor. | 23/05/2016 | 7.2 | CVE-2016-4557 |
| PHP | The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. | 21/05/2016 | 7.5 | CVE-2016-4544 |
| PHP | The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. | 21/05/2016 | 7.5 | CVE-2016-4543 |
| PHP | The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. | 21/05/2016 | 7.5 | CVE-2016-4542 |
| PHP | The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset. | 21/05/2016 | 7.5 | CVE-2016-4541 |
| PHP | The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset. | 21/05/2016 | 7.5 | CVE-2016-4540 |
| PHP | The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero. | 21/05/2016 | 7.5 | CVE-2016-4539 |
| PHP | The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call. | 21/05/2016 | 7.5 | CVE-2016-4538 |
| PHP | The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call. | 21/05/2016 | 7.5 | CVE-2016-4537 |
| PHP | Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow. | 21/05/2016 | 7.5 | CVE-2016-4346 |
| PHP | Integer overflow in the php_filter_encode_url function in ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow. | 21/05/2016 | 7.5 | CVE-2016-4345 |
| PHP | Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading to a heap-based buffer overflow. | 21/05/2016 | 7.5 | CVE-2016-4344 |
| PHP | ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive. | 21/05/2016 | 8.3 | CVE-2016-4342 |
| PHP | Double free vulnerability in the format printer in PHP 7.x before 7.0.1 allows remote attackers to have an unspecified impact by triggering an error. | 21/05/2016 | 10.0 | CVE-2015-8880 |
| PHP | Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data. | 21/05/2016 | 7.5 | CVE-2015-8876 |

Semana 16/05/2016

| Primeiro Vendor – Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| PHP | The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in ext/phar/phar.c. | 20/05/2016 | 7.5 | CVE-2016-4072 |
| PHP | Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call. | 20/05/2016 | 7.5 | CVE-2016-4071 |
| Apple--mac | The NVIDIA Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1846 |
| Apple--mac | The kernel in Apple iOS before 9.3.2 and OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1831 |
| Apple--mac | The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1827, CVE-2016-1828, and CVE-2016-1829. | 20/05/2016 | 8.5 | CVE-2016-1830 |
| Apple--mac | The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1827, CVE-2016-1828, and CVE-2016-1830. | 20/05/2016 | 8.5 | CVE-2016-1829 |
| Apple--mac | The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1827, CVE-2016-1829, and CVE-2016-1830. | 20/05/2016 | 9.3 | CVE-2016-1828 |
| Apple--mac | The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1828, CVE-2016-1829, and CVE-2016-1830. | 20/05/2016 | 9.3 | CVE-2016-1827 |
| Apple--mac | Integer overflow in the ptrace implementation in the kernel in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1826 |
| Apple--mac | IOHIDFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1825 |
| Apple--tv | IOHIDFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1823. | 20/05/2016 | 9.3 | CVE-2016-1824 |
| Apple--mac | IOHIDFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1824. | 20/05/2016 | 9.3 | CVE-2016-1823 |
| Apple--mac | IOFireWireFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1822 |
| Apple--mac | IOAudioFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1821 |
| Apple--mac | Buffer overflow in IOAudioFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1820 |
| Apple--mac | IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1817 and CVE-2016-1818. | 20/05/2016 | 9.3 | CVE-2016-1819 |
| Apple--iphone | IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1817 and CVE-2016-1819. | 20/05/2016 | 9.3 | CVE-2016-1818 |
| Apple--mac | IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 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-2016-1818 and CVE-2016-1819. | 20/05/2016 | 9.3 | CVE-2016-1817 |
| Apple--mac | IOAcceleratorFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1816 |
| Apple--mac | IOAcceleratorFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1815 |
| Apple--mac | IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1813 |
| Apple--mac | Buffer overflow in Intel Graphics Driver in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1812 |
| Apple--mac | The Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1810 |
| Apple--mac | Disk Utility in Apple OS X before 10.11.5 uses incorrect encryption keys for disk images, which has unspecified impact and attack vectors. | 20/05/2016 | 7.8 | CVE-2016-1809 |
| Apple--watchos | The Disk Images subsystem in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1808 |
| Apple--mac | Crash Reporter in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1806 |
| Apple--mac | CoreStorage in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1805 |
| Apple--mac | The Multi-Touch subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1804 |
| Apple--mac | CoreCapture in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1803 |
| Apple--mac | Captive Network Assistant in Apple OS X before 10.11.5 mishandles a custom URL scheme, which allows user-assisted remote attackers to execute arbitrary code via unspecified vectors. | 20/05/2016 | 9.3 | CVE-2016-1800 |
| Apple--mac | Audio in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1799 |
| Apple--mac | Apple Type Services (ATS) in Apple OS X before 10.11.5 allows attackers to bypass intended FontValidator sandbox policy restrictions and execute arbitrary code in a privileged context via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1797 |
| Apple--mac | AppleGraphicsPowerManagement in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1795 |
| Apple--mac | AppleGraphicsControl in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app, a different vulnerability than CVE-2016-1793. | 20/05/2016 | 9.3 | CVE-2016-1794 |
| Apple--mac | AppleGraphicsControl in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app, a different vulnerability than CVE-2016-1794. | 20/05/2016 | 9.3 | CVE-2016-1793 |
| Apple--mac | The AMD subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. | 20/05/2016 | 9.3 | CVE-2016-1792 |
| Apple--itunes | Untrusted search path vulnerability in the installer in Apple iTunes before 12.4 allows local users to gain privileges via a Trojan horse DLL in the current working directory. | 20/05/2016 | 7.2 | CVE-2016-1747 |
| Symantec--antivirus | The kernel component in Symantec Anti-Virus Engine (AVE) 20151.1 before 20151.1.1.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory access violation and system crash) via a malformed PE header file. | 19/05/2016 | 9.4 | CVE-2016-2208 |
| Xen | The guest_walk_tables function in arch/x86/mm/guest_walk.c in Xen 4.6.x and earlier does not properly handle the Page Size (PS) page table entry bit at the L4 and L3 page table levels, which might allow local guest OS users to gain privileges via a crafted mapping of memory. | 18/05/2016 | 7.2 | CVE-2016-4480 |
| Vmware--Player | VMware Workstation 11.x before 11.1.3 and VMware Player 7.x before 7.1.3 on Windows incorrectly access an executable file, which allows host OS users to gain host OS privileges via unspecified vectors. | 18/05/2016 | 10.0 | CVE-2016-2077 |
| PHP | Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive. | 16/05/2016 | 10.0 | CVE-2016-2554 |
| PHP | The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed __cookies array, related to the SoapClient::__call method in ext/soap/soap.c. | 16/05/2016 | 7.5 | CVE-2015-8835 |
| PHP | The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content. | 16/05/2016 | 7.5 | CVE-2015-6835 |
| PHP | Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization. | 16/05/2016 | 7.5 | CVE-2015-6834 |
| PHP | The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call. | 16/05/2016 | 10.0 | CVE-2015-5589 |
| PHP | Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6022. | 16/05/2016 | 7.5 | CVE-2015-4643 |
| PHP | The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function. | 16/05/2016 | 10.0 | CVE-2015-4642 |
| PHP | The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue. | 16/05/2016 | 10.0 | CVE-2015-4603 |
| PHP | The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue. | 16/05/2016 | 10.0 | CVE-2015-4602 |
| PHP | PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600. | 16/05/2016 | 10.0 | CVE-2015-4601 |
| PHP | The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods. | 16/05/2016 | 10.0 | CVE-2015-4600 |
| PHP | The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue. | 16/05/2016 | 10.0 | CVE-2015-4599 |
| PHP | PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagesx/loadfont function, as demonstrated by a filename=0.html attack that bypasses an intended configuration in which client users may write to only .html files. | 16/05/2016 | 7.5 | CVE-2015-4598 |
| PHP | Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation. | 16/05/2016 | 7.5 | CVE-2015-4116 |

# Histórico de vulnerabilidades de Maio do 2016

## Semana 09/05/2016

| Primeiro Vendor – Product | Description | Published | CVSs Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | |
| Google--Chrome | The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code. | 14/05/2016 | 9.3 | CVE-2016-1669 |
| Google--Chrome | Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. | 14/05/2016 | 7.5 | CVE-2016-1666 |
| Google--Chrome | extensions/renderer/gc_callback.cc in Google Chrome before 50.0.2661.94 does not prevent fallback execution once the Garbage Collection callback has started, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors. | 14/05/2016 | 10.0 | CVE-2016-1667 |
| Google--Chrome | Blink, as used in Google Chrome before 50.0.2661.94, does not ensure that frames satisfy a check for the same renderer process in addition to a Same Origin Policy check, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted web site, related to BindingSecurity.cpp and DOMWindow.cpp. | 14/05/2016 | 9.3 | CVE-2016-1661 |
| Meteocontrol--web | Meteocontrol WEB'log Basic 100, Light, Pro, and Pro Unlimited allows remote attackers to obtain sensitive cleartext information via unspecified vectors. | 14/05/2016 | 10.0 | CVE-2016-2294 |
| Meteocontrol--web | Meteocontrol WEB'log Basic 100, Light, Pro, and Pro Unlimited allows remote attackers to execute arbitrary commands via an "access command shell like feature. | 14/05/2016 | 9.7 | CVE-2016-2297 |
| Meteocontrol--web | Meteocontrol WEB'log Basic 100, Light, Pro, and Pro Unlimited does not require authentication for "post-admin" login pages, which allows remote attackers to obtain sensitive information or modify data via unspecified vectors. | 14/05/2016 | 7.5 | CVE-2016-2296 |
| Ninjaforms | The Ninja Forms plugin before 2.9.42.1 for WordPress allows remote attackers to conduct PHP object injection attacks via crafted serialized values in a POST request. | 14/05/2016 | 7.5 | CVE-2016-1309 |
| Symantec--endpoint | Unquoted Windows search path vulnerability in EIDService in Symantec Endpoint Encryption (SEE) 11.x before 11.1.1 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory, as demonstrated by program.exe. | 13/05/2016 | 7.2 | CVE-2015-8156 |
| Botan--Project | The BER decoder in Botan 1.10.x before 1.10.10 and 1.11.x before 1.11.19 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors, related to a length field. | 13/05/2016 | 7.8 | CVE-2015-5727 |
| Sap--netweaver | The Invoker Servlet on SAP NetWeaver Application Server Java platforms, possibly before 7.3, does not require authentication, which allows remote attackers to execute arbitrary code via an HTTP or HTTPS request, as exploited in the wild in 2013 through 2016, aka a "Detour" attack. | 13/05/2016 | 10.0 | CVE-2010-5326 |
| Debian--Linux | Integer overflow in mtlib2 before 1.4.9 on 32-bit platforms allows remote attackers to execute arbitrary code via large dimensions in an image, which triggers an out-of-bounds heap memory write operation. | 13/05/2016 | 7.5 | CVE-2016-8024 |
| Botan--Project | Heap-based buffer overflow in the P-521 reduction function in Botan 1.11.x before 1.11.27 allows remote attackers to cause a denial of service (memory overwrite and crash) or execute arbitrary code via unspecified vectors. | 13/05/2016 | 10.0 | CVE-2016-2195 |
| Debian--Linux | Integer overflow in the PointGFp constructor in Botan before 1.10.11 and 1.11.x before 1.11.27 allows remote attackers to overwrite memory and possibly execute arbitrary code via a crafted ECC point, which triggers a heap-based buffer overflow. | 13/05/2016 | 10.0 | CVE-2016-2195 |
| Debian--Linux | The VGA module in QEMU improperly performs bounds checking on banked access to video memory, which allows local guest OS users to execute arbitrary code on the host by changing access modes after setting the bank register, aka the "Dark Portal" issue. | 11/05/2016 | 7.2 | CVE-2016-3710 |
| Microsoft--Edge | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4116 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4115 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4114 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4113 |
| Adobe--Flashplayer | respectified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4112 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4111 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4110 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4109 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-4108 |
| Adobe--acrobat | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, and CVE-2016-4102. | 11/05/2016 | 10.0 | CVE-2016-4107 |
| Adobe--Reader | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-1090. | 11/05/2016 | 7.2 | CVE-2016-4106 |
| Adobe--acrobat | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, and CVE-2016-4104. | 11/05/2016 | 10.0 | CVE-2016-4105 |
| Adobe--acrobat | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4104 |
| Adobe--acrobat dc | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-4102 |
| Adobe--acrobat | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4101 |
| Adobe--Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, and CVE-2016-4104. | 11/05/2016 | 10.0 | CVE-2016-4102 |
| Adobe--Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4103 |
| Adobe--Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4098 |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4097 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4096 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4094 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4093 |
| Adobe-Reader DC | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4091. | 11/05/2016 | 10.0 | CVE-2016-4092 |
| Adobe-Reader DC | Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4092. | 11/05/2016 | 10.0 | CVE-2016-4091 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4095 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4086 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-4088 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1130 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1128 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1127 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1126 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1125 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1134 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1121 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1122 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1121 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1120 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1119 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1118 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, and CVE-2016-1092. | 11/05/2016 | 10.0 | CVE-2016-1117 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1116 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information via unspecified vectors. | 11/05/2016 | 10.0 | CVE-2016-1117 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1085 |

# Histórico de vulnerabilidades de Maio do 2016

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1061 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1093 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1088 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1089 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1085 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1084 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1083 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1082 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1081 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1080 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1078 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1077 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1076 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1075 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1074 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1073 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1072 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1071 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1070 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1069 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1068 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1067 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1066 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1065 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1064 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1037, CVE-2016-1054, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1063 |

| | | | | |
|---|---|---|---|---|
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1062 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1061 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1060 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1059 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1058 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1057 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1056 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1055 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1054 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1053 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1052 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1051 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1050 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1049 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1048 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1047 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1046 |
| Adobe-Reader | Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, and CVE-2016-4107. | 11/05/2016 | 10.0 | CVE-2016-1045 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1044 |
| Adobe-Reader | Integer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. | 11/05/2016 | 10.0 | CVE-2016-1043 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1043, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1042 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1042, CVE-2016-1043, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1041 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1041, CVE-2016-1042, CVE-2016-1043, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1040 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1043, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1039 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1043, CVE-2016-1062, and CVE-2016-1117. | 11/05/2016 | 10.0 | CVE-2016-1038 |
| Adobe-Reader | Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 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-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. | 11/05/2016 | 10.0 | CVE-2016-1037 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1110 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1109 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1108 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1107 |

# Histórico de vulnerabilidades de Maio do 2016

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1096 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1095 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1094 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1093 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1092 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1101 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1100 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1099 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1098 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1097 |
| Adobe--Flashplayer | Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. | 11/05/2016 | 7.6 | CVE-2016-1096 |
| Adobe-Reader | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-4106. | 11/05/2016 | 7.2 | CVE-2016-1090 |
| Adobe-Reader | Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1090 and CVE-2016-4106. | 11/05/2016 | 7.2 | CVE-2016-1087 |
| Adobe--Flashplayer | Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in May 2016. | 10/05/2016 | 10.0 | CVE-2016-4117 |
| Adobe--coldfusion | Adobe ColdFusion 10 before Update 19, 11 before Update 8, and 2016 before Update 1 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. | 10/05/2016 | 7.5 | CVE-2016-1114 |
| 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, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0198 |
| Microsoft--windows | dxgkrnl.sys in the DirectX Graphics kernel subsystem in 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 allows local users to gain privileges via a crafted application, aka "Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability." | 10/05/2016 | 7.2 | CVE-2016-0197 |
| 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," a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0174. | 10/05/2016 | 7.2 | CVE-2016-0196 |
| Microsoft--windows | The Imaging Component 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 document, aka "Windows Imaging Component Memory Corruption Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0195 |
| Microsoft--edge | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0191. | 10/05/2016 | 7.6 | CVE-2016-0193 |
| 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." | 10/05/2016 | 7.6 | CVE-2016-0192 |
| Microsoft--edge | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0193. | 10/05/2016 | 7.6 | CVE-2016-0191 |
| Microsoft--internetexplorer | The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0187. | 10/05/2016 | 7.6 | CVE-2016-0189 |
| Microsoft--internetexplorer | The User Mode Code Integrity (UMCI) implementation in Device Guard in Microsoft Internet Explorer 11 allows remote attackers to bypass a code-signing protection mechanism via unspecified vectors, aka "Internet Explorer Security Feature Bypass." | 10/05/2016 | 9.3 | CVE-2016-0188 |
| Microsoft--vbscript | The Microsoft (1) JScript 5.8 and (2) VBScript 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0189. | 10/05/2016 | 7.6 | CVE-2016-0187 |
| Microsoft--edge | The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0191 and CVE-2016-0193. | 10/05/2016 | 7.6 | CVE-2016-0186 |
| Microsoft--windows | Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted Media Center link (aka .mcl) file, aka "Windows Media Center Remote Code Execution Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0185 |
| Microsoft--windows | Use-after-free vulnerability in GDI 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 document, aka "DirectED Use-After-Free Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0184 |
| Microsoft--office | The Windows font library in Microsoft Office 2010 SP2, Word 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Microsoft Office Graphics RCE Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0183 |
| Microsoft--windows | Windows Journal in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal (aka .jnt) file, aka "Windows Journal Memory Corruption Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0182 |
| Microsoft--windows | The kernel 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 mishandles symbolic links, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." | 10/05/2016 | 7.2 | CVE-2016-0180 |
| Microsoft--windows | Windows Shell in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Shell Remote Code Execution Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0179 |
| Microsoft--windows | The RPC NDR Engine 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 mishandles free operations, which allows remote attackers to execute arbitrary code via malformed RPC requests, aka "RPC Network Data Representation Engine Elevation of Privilege Vulnerability." | 10/05/2016 | 9.0 | CVE-2016-0178 |
| Microsoft--windows | dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 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 "Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability." | 10/05/2016 | 7.2 | CVE-2016-0176 |
| 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," a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0196. | 10/05/2016 | 7.2 | CVE-2016-0175 |
| 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," a different vulnerability than CVE-2016-0171, CVE-2016-0174, and CVE-2016-0196. | 10/05/2016 | 7.2 | CVE-2016-0173 |
| 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," a different vulnerability than CVE-2016-0173, CVE-2016-0174, and CVE-2016-0196. | 10/05/2016 | 7.2 | CVE-2016-0171 |
| Microsoft--windows | GDI 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 document, aka "Windows Graphics Component RCE Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0170 |
| Microsoft--windows | Internet Information Services (IIS) in Microsoft Windows Vista SP2 and Server 2008 SP2 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows DLL Loading Remote Code Execution Vulnerability." | 10/05/2016 | 7.2 | CVE-2016-0152 |
| Microsoft--office | Microsoft Office 2007 SP3, Office 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0140 |
| Microsoft--office | Microsoft Office 2013 SP1, 2013 RT SP1, and 2016 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." | 10/05/2016 | 9.3 | CVE-2016-0126 |
| Solarwinds--storage | Multiple SQL injection vulnerabilities in the Web Services web server in SolarWinds Storage Resource Monitor (SRM) Profiler (formerly Storage Manager (STM)) before 6.2.3 allow remote attackers to execute arbitrary SQL commands via the (1) ScriptSchedule parameter in the ScriptServlet servlet; the (2) winEventId or (3) winEventLog parameter in the WindowsEventLogsServlet servlet; the (4) processOS parameter in the ProcessesServlet servlet; the (5) group, (6) groupName, or (7) clientName parameter in the BackupExceptionsServlet servlet; the (8) vatDB or (9) vatFS parameter in the BackupAssociationServlet servlet; the (10) orderBy or (11) orderDir parameter in the HostStorageServlet servlet; the (12) fileName, (13) sortField, or (14) sortDirection parameter in the DuplicateFilesServlet servlet; the (15) orderFld or (16) orderDir parameter in the QuantumMonitorServlet servlet; the (17) exitCode parameter in the NbuErrorMessageServlet servlet; the (18) udfName, (19) displayName, (20) udfDescription, (21) udfDataValue, (22) udfSectionName, or (23) udfId parameter in the UserDefinedFieldConfigServlet servlet; the (24) sortField or (25) sortDirection parameter in the KioteckMonitorServlet servlet; the (26) sortField or (27) sortDirection parameter in the BesDriveUsageSummaryServlet servlet. | 09/05/2016 | 10.0 | CVE-2016-4350 |
| Google--Android | OpenSSLCipher.java in Conscrypt in Android 6.x before 2016-05-01 mishandles updates of the Additional Authenticated Data (AAD) array, which allows attackers to spoof message authentication via unspecified vectors, aka internal bug 27371173. | 09/05/2016 | 7.6 | CVE-2016-2482 |
| Google--Android | OpenSSLCipher.java in Conscrypt in Android 6.x before 2016-05-01 mishandles resets of the Additional Authenticated Data (AAD) array, which allows attackers to spoof message authentication via unspecified vectors, aka internal bugs 27324690 and 27696681. | 09/05/2016 | 7.6 | CVE-2016-2481 |
| Google--Android | The MediaTek Wi-Fi driver in Android before 2016-05-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 27549705. | 09/05/2016 | 7.6 | CVE-2016-2479 |
| Google--Android | codecs/amrnb/dec/SoftAMR.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bugs 27662364 and 27661673. | 09/05/2016 | 9.3 | CVE-2016-2412 |

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | |
| Google--Android | codecs/on2/dec/SoftVPX.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate VPX output buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27597103. | 09/05/2016 | 9.3 | CVE-2016-2451 |
| Google--Android | codecs/on2/enc/SoftVPXEncoder.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate OMX buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27569635. | 09/05/2016 | 9.3 | CVE-2016-2450 |
| Google--Android | services/camera/libcameraservice/device3/Camera3Device.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate template IDs, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27568958. | 09/05/2016 | 9.3 | CVE-2016-2449 |
| Google--Android | media/libmediaplayerservice/nuplayer/RtpPlayerStreamListener.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not properly validate entry data structures, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27533704. | 09/05/2016 | 9.3 | CVE-2016-2448 |
| Google--Nexus | The NVIDIA media driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27441354. | 09/05/2016 | 7.6 | CVE-2016-2446 |
| Google--Nexus | The NVIDIA media driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27253079. | 09/05/2016 | 7.6 | CVE-2016-2445 |
| Google--Nexus | The NVIDIA media driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27209332. | 09/05/2016 | 7.6 | CVE-2016-2444 |
| Google--Nexus | The Qualcomm MDP driver in Android before 2016-05-01 on Nexus 5 and Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 26604525. | 09/05/2016 | 7.6 | CVE-2016-2443 |
| Google--Nexus | The Qualcomm buspm driver in Android before 2016-05-01 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 26464907. | 09/05/2016 | 9.3 | CVE-2016-2442 |
| Google--Nexus | he Qualcomm buspm driver in Android before 2016-05-01 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 26354602. | 09/05/2016 | 9.3 | CVE-2016-2441 |
| Google--Android | libs/binder/IPCThreadState.cpp in Binder in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 mishandles object references, which allows attackers to gain privileges via a crafted application, aka internal bug 27252696. | 09/05/2016 | 9.3 | CVE-2016-2440 |
| Google--Nexus | The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27436822. | 09/05/2016 | 9.3 | CVE-2016-2437 |
| Google--Nexus | The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27292611. | 09/05/2016 | 9.3 | CVE-2016-2436 |
| Google--Nexus | The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27297888. | 09/05/2016 | 9.3 | CVE-2016-2435 |
| Google--Nexus | The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27252060. | 09/05/2016 | 9.3 | CVE-2016-2434 |
| Google--Nexus | The Qualcomm TrustZone component in Android before 2016-05-01 on Nexus 6 and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 25913059. | 09/05/2016 | 9.3 | CVE-2016-2433 |
| Google--Nexus | The Qualcomm TrustZone component in Android before 2016-05-01 on Nexus 5, Nexus 6, Nexus 7 (2013), and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 24968809. | 09/05/2016 | 9.3 | CVE-2016-2431 |
| Google--Android | libbacktrace/Backtrace.cpp in debuggerd in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 allows attackers to gain privileges via an application containing a crafted symbol name, aka internal bug 27299236. | 09/05/2016 | 9.3 | CVE-2016-2430 |
| Google--Android | librLAC/stream_decoder.c in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not prevent free operations on uninitialized memory, which allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted media file, aka internal bug 27211885. | 09/05/2016 | 10.0 | CVE-2016-2429 |
| Google--Android | libAACenc/src/aacenc_rom.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016- | 09/05/2016 | 10.0 | CVE-2016-2428 |
| Google--Android | server/TetherController.cpp in the tethering controller in netd, as distributed with Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly validate upstream interface names, which allows attackers to bypass intended access restrictions via a crafted application. | 09/05/2016 | 9.3 | CVE-2016-2062 |
| Linux | The WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify authorization for private SET IOCTL calls, which allows attackers to gain privileges via a crafted application, related to wlan_hdd_hostapd.c and wlan_hdd_wext.c. | 09/05/2016 | 9.3 | CVE-2015-0571 |
| Linux | Stack-based buffer overflow in the SET_WPS_IE IOCTL implementation in wlan_hdd_hostapd.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges via a crafted application that uses a long WPS IE element. | 09/05/2016 | 9.3 | CVE-2015-0570 |
| Linux | Heap-based buffer overflow in the private wireless extensions IOCTL implementation in wlan_hdd_wext.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges via a crafted application that establishes a packet filter. | 09/05/2016 | 9.3 | CVE-2015-0569 |

**Semana 02/05/2016**

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Canonical--ubuntu | Heap-based buffer overflow in the ExponentialFunction::ExponentialFunction function in Poppler before 0.40.0 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via an invalid blend mode in the ExtGState dictionary in a crafted PDF document. | 06/05/2016 | 9.3 | CVE-2015-8868 |
| Debian--Linux | Cool Projects TarDiff allows remote attackers to execute arbitrary commands via shell metacharacters in the name of a (1) tar file or (2) file within a tar file. | 06/05/2016 | 10.0 | CVE-2015-0857 |
| Imagemagick | The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via a crafted image. | 05/05/2016 | 7.1 | CVE-2016-3717 |
| Imagemagick | The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick." | 05/05/2016 | 10.0 | CVE-2016-3714 |
| Cisco--telepresence | The XML API in TelePresence Codec (TC) 7.2.0, 7.2.1, 7.3.0, 7.3.1, 7.3.2, 7.3.3, 7.3.4, and 7.3.5 and Collaboration Endpoint (CE) 8.0.0, 8.0.1, and 8.1.0 in Cisco TelePresence Software mishandles authentication, which allows remote attackers to execute control commands or make configuration changes via an API request, aka Bug ID CSCvc26935. | 05/05/2016 | 9.0 | CVE-2016-1387 |
| Openssl | The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding. | 04/05/2016 | 7.8 | CVE-2016-2109 |
| Openssl | The ASN.1 implementation in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue. | 04/05/2016 | 10.0 | CVE-2016-2108 |
| Linux--kernel | The tcp_cwnd_reduction function in net/ipv4/tcp_input.c in the Linux kernel before 4.3.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via crafted TCP traffic. | 02/05/2016 | 7.8 | CVE-2016-2059 |
| Linux--kernel | The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c. | 02/05/2016 | 7.1 | CVE-2016-2053 |
| Canonical--ubuntu | The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program. | 02/05/2016 | 7.2 | CVE-2016-1576 |
| Canonical--ubuntu | The overlayfs implementation in the Linux kernel through 4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory. | 02/05/2016 | 7.2 | CVE-2016-1575 |
| Linux--kernel | Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression. | 02/05/2016 | 7.2 | CVE-2015-8830 |
| Linux--kernel | The skb_copy_and_csum_datagram_iovec function in net/core/datagram.c in the Linux kernel 3.14.54 and 3.18.22 does not accept a length argument, which allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write system call followed by a recvmsg system call. | 02/05/2016 | 7.2 | CVE-2015-8019 |
| Linux--kernel | net/socket.c in the Linux kernel 3.19 before 3.19.3 does not validate certain range data for (1) sendto and (2) recvfrom system calls, which allows local users to gain privileges by leveraging a subsystem that uses the copy_from_iter function in the iov_iter interface, as demonstrated by the Bluetooth subsystem. | 02/05/2016 | 7.2 | CVE-2015-2686 |
| Linux--kernel | Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. | 02/05/2016 | 7.2 | CVE-2012-6701 |
| Linux--kernel | The netlink_sendmsg function in net/netlink/af_netlink.c in the Linux kernel before 3.5.5 does not validate the dst_pid field, which allows local users to have an unspecified impact by spoofing Netlink messages. | 02/05/2016 | 7.2 | CVE-2012-6689 |
| Linux--kernel | The redirect_target function in net/ipv4/netfilter/ipt_REDIRECT.c in the Linux kernel before 2.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and DOPS) by sending packets to an interface that has a 0.0.0.0 IP address, a related issue to CVE-2015-8787. | 02/05/2016 | 7.8 | CVE-2003-1604 |
| Debian--Linux | The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable. | 30/04/2016 | 7.2 | CVE-2015-8325 |
| Mozilla--firefox | Unspecified vulnerability in the browser engine in Mozilla Firefox ESR 38.x before 38.8 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. | 30/04/2016 | 10.0 | CVE-2016-2805 |
| Mozilla--firefox | Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0 and Firefox ESR 45.x before 45.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. | 30/04/2016 | 10.0 | CVE-2016-2806 |
| Mozilla--firefox | Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0, Firefox ESR 38.x before 38.8, and Firefox ESR 45.x before 45.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. | 30/04/2016 | 10.0 | CVE-2016-2807 |