Histórico de vulnerabilidades de Octubre del 2016

Semana 24/10/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to apply a message filter that contains certain rules. More Information: CSCux59873. Known Affected Releases: 8.5.6-106 9.1.0-032 9.7.0-125. Known Fixed Releases: 9.1.1-038 9.7.1-066.	28/10/2016	7.8	CVE-2016-1481
cisco -- email_security_appliance	A vulnerability in the email attachment scanning functionality of the Advanced Malware Protection (AMP) feature of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to cause an affected device to stop scanning and forwarding email messages due to a denial of service (DoS) condition. Affected Products: This vulnerability affects Cisco AsyncOS Software releases 9.7.1 and later, prior to the first fixed release, for both virtual and hardware Cisco Email Security Appliances, if the AMP feature is configured to scan incoming email attachments. More Information: CSCuy99453. Known Affected Releases: 9.7.1-066. Known Fixed Releases: 10.0.0-125 9.7.1-207 9.7.2-047.	28/10/2016	7.8	CVE-2016-1486
cisco -- email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to cause an affected device to stop scanning and forwarding email messages due to a denial of service (DoS) condition. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to apply a message filter or content filter to incoming email attachments. The vulnerability is not limited to any specific rules or actions for a message filter or content filter. More Information: CSCuz63143. Known Affected Releases: 8.5.7-042 9.7.0-125. Known Fixed Releases: 10.0.0-125 9.1.1-038 9.7.2-047.	28/10/2016	7.8	CVE-2016-6356
cisco -- ip_interoperability_and_collaboration_system	A vulnerability in the interdevice communications interface of the Cisco IP Interoperability and Collaboration System (IPICS) Universal Media Services (UMS) could allow an unauthenticated, remote attacker to modify configuration parameters of the UMS and cause the system to become unavailable. Affected Products: This vulnerability affects Cisco IPICS releases 4.8(1) to 4.10(1). More Information: CSCva46644. Known Affected Releases: 4.10(1) 4.8(1) 4.8(2) 4.9(1) 4.9(2).	28/10/2016	10.0	CVE-2016-6397
libcsp_project -- libcsp	Buffer overflow in the csp_can_process_frame in csp_if_can.c in the libcsp library v1.4 and earlier allows hostile components connected to the canbus to execute arbitrary code via a long csp packet.	28/10/2016	7.5	CVE-2016-8596
libcsp_project -- libcsp	Buffer overflow in the csp_sfp_recv_fp in csp_sfp.c in the libcsp library v1.4 and earlier allows hostile components with network access to the SFP underlying network layers to execute arbitrary code via specially crafted SFP packets.	28/10/2016	7.5	CVE-2016-8597
cisco -- adaptive_security_appliance	A vulnerability in the local Certificate Authority (CA) feature of Cisco ASA Software before 9.6(1.5) could allow an unauthenticated, remote attacker to cause a reload of the affected system. The vulnerability is due to improper handling of crafted packets during the enrollment operation. An attacker could exploit this vulnerability by sending a crafted enrollment request to the affected system. An exploit could allow the attacker to cause the reload of the affected system. Note: Only HTTPS packets directed to the Cisco ASA interface, where the local CA is allowing user enrollment, can be used to trigger this vulnerability. This vulnerability affects systems configured in routed firewall mode and in single or multiple context mode.	27/10/2016	7.1	CVE-2016-6431
apache -- commons_fileupload	Apache Commons FileUpload DiskFileItem File Manipulation Remote Code Execution	25/10/2016	7.5	CVE-2016-1000031
oracle -- weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to JavaServer Faces.	25/10/2016	9.0	CVE-2016-3505
oracle -- weblogic_server	Unspecified vulnerability in the Oracle Web Services component in Oracle Fusion Middleware 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, and 12.2.1.0.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAXWS Web Services Stack.	25/10/2016	10.0	CVE-2016-3551
oracle -- istore	Unspecified vulnerability in the Oracle iStore component in Oracle E-Business Suite 12.1.1 through 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality and integrity via vectors related to Runtime Catalog.	25/10/2016	7.8	CVE-2016-5489
oracle -- vm_virtualbox	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality, integrity, and availability via vectors related to Core, a different vulnerability than CVE-2016-5538.	25/10/2016	7.2	CVE-2016-5501
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality and integrity via unknown vectors, a different vulnerability than CVE-2016-5512.	25/10/2016	7.5	CVE-2016-5521
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Apache Tomcat.	25/10/2016	7.5	CVE-2016-5526
oracle -- weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS-WebServices.	25/10/2016	7.5	CVE-2016-5531
oracle -- weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, 12.2.1.0, and 12.2.1.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	25/10/2016	7.5	CVE-2016-5535
oracle -- vm_virtualbox	Unspecified vulnerability in the Oracle VM VirtualBox component before 5.0.28 and 5.1.x before 5.1.8 in Oracle Virtualization allows local users to affect confidentiality, integrity, and availability via vectors related to Core, a different vulnerability than CVE-2016-5501.	25/10/2016	7.2	CVE-2016-5538
oracle -- solaris	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.3 allows local users to affect confidentiality, integrity, and availability via vectors related to Kernel/X86.	25/10/2016	7.2	CVE-2016-5544
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D.	25/10/2016	9.3	CVE-2016-5556
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588.	25/10/2016	7.5	CVE-2016-5558
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT.	25/10/2016	9.3	CVE-2016-5568
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5577, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588.	25/10/2016	7.5	CVE-2016-5574
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5578, CVE-2016-5579, and CVE-2016-5588.	25/10/2016	7.5	CVE-2016-5577
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5579, and CVE-2016-5588.	25/10/2016	7.5	CVE-2016-5578
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, and CVE-2016-5588.	25/10/2016	7.5	CVE-2016-5579
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5573.	25/10/2016	9.3	CVE-2016-5582
oracle -- outside_in_technology	Unspecified vulnerability in the Oracle Outside In Technology component in Oracle Fusion Middleware 8.4.0 and 8.5.1 through 8.5.3 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Outside In Filters, a different vulnerability than CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, and CVE-2016-5579.	25/10/2016	7.5	CVE-2016-5588
oracle -- flexcube_universal_banking	Unspecified vulnerability in the Oracle FLEXCUBE Universal Banking component in Oracle Financial Services Applications 11.3.0, 11.4.0, 12.0.1 through 12.0.3, 12.1.0, and 12.2.0 allows remote attackers to affect confidentiality and integrity via vectors related to INFRA.	25/10/2016	7.8	CVE-2016-5622
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7853, and CVE-2016-7854.	21/10/2016	10.0	CVE-2016-7852
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7854.	21/10/2016	10.0	CVE-2016-7853
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019, CVE-2016-7852, and CVE-2016-7853.	21/10/2016	10.0	CVE-2016-7854
ibm -- security_guardium_database_activity_monitor	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote authenticated users to execute arbitrary commands with root privileges via the search field.	21/10/2016	9.0	CVE-2016-0236
ibm -- security_guardium_database_activity_monitor	IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows local users to obtain administrator privileges for command execution via unspecified vectors.	21/10/2016	7.2	CVE-2016-0328

Semana 17/10/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_guardium	SQL injection vulnerability in IBM Security Guardium Database Activity Monitor 8.2 before p310, 9.x through 9.5 before p700, and 10.x through 10.1 before p100 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	16/10/2016	7.5	CVE-2016-0249
linux -- linux_kernel	mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero.	16/10/2016	7.2	CVE-2015-3288
linux -- linux_kernel	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.	16/10/2016	7.8	CVE-2016-7039
linux -- linux_kernel	The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code.	16/10/2016	7.2	CVE-2016-7425
linux -- linux_kernel	The IP stack in the Linux kernel before 4.6 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039.	16/10/2016	7.8	CVE-2016-8666

Semana 10/10/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-1089
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-1091
adobe -- flash_player	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.	13/10/2016	10.0	CVE-2016-4286
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6940
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6941
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6942
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6943
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6944
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6945
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6946
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6947
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6948
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6949
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6950
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6951
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6952
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6953
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6954
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6955

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6956
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors.	13/10/2016	10.0	CVE-2016-6957
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to bypass intended access restrictions via unspecified vectors.	13/10/2016	10.0	CVE-2016-6958
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6959
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6960
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6961
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6962
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6963
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6964
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6965
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6966
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6967
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6968
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6969
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6970
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6979, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6971
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6972
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6973
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6974
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6975
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6976

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6977
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6978
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6988, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6979
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and CVE-2016-6993.	13/10/2016	10.0	CVE-2016-6988
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, and CVE-2016-6988.	13/10/2016	10.0	CVE-2016-6993
adobe -- acrobat	Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6939.	13/10/2016	10.0	CVE-2016-6994
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6995
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6996
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6997
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-6998
adobe -- acrobat	Integer overflow in Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	13/10/2016	10.0	CVE-2016-6999
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7000
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7001
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7002
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7003
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7004
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7005
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7006

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7007
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7008
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7009
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7010
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7011
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7012
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7013
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7014
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7015
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7017, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7016
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7018, and CVE-2016-7019.	13/10/2016	10.0	CVE-2016-7017
apache -- tomcat	The Tomcat package on Red Hat Enterprise Linux (RHEL) 5 through 7, JBoss Web Server 3.0, and JBoss EWS 2 uses weak permissions for (1) /etc/sysconfig/tomcat and (2) /etc/tomcat/tomcat.conf, which allows local users to gain privileges by leveraging membership in the tomcat group.	13/10/2016	7.2	CVE-2016-6325
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	13/10/2016	9.3	CVE-2016-3331
microsoft -- edge	The scripting engines in 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, as demonstrated by the Chakra JavaScript engine, aka "Scripting Engine Memory Corruption Vulnerability."	13/10/2016	9.3	CVE-2016-3382
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows 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."	13/10/2016	9.3	CVE-2016-3383
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	13/10/2016	9.3	CVE-2016-3384
microsoft -- internet_explorer	The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	13/10/2016	9.3	CVE-2016-3385
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-2016-3389, CVE-2016-7190, and CVE-2016-7194.	13/10/2016	9.3	CVE-2016-3386
microsoft -- edge	Microsoft Internet Explorer 10 and 11 and Microsoft Edge do not properly restrict access to private namespaces, which allows remote attackers to gain privileges via unspecified vectors, aka "Microsoft Browser Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3387.	13/10/2016	9.3	CVE-2016-3388
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Remote Code Execution Vulnerability."	13/10/2016	9.3	CVE-2016-7189
canonical -- ubuntu_linux	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.	10/10/2016	10.0	CVE-2016-7117
google -- android	Multiple use-after-free vulnerabilities in sound/soc/msm/qdsp6v2/msm-lsm-client.c in the Qualcomm sound driver in Android before 2016-10-05 on Nexus 5X, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 30142668 and Qualcomm internal bug CR 948902.	10/10/2016	9.3	CVE-2015-8951
google -- android	cmds/servicemanager/service_manager.c in ServiceManager in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not properly restrict service registration, which allows attackers to gain privileges via a crafted application, aka internal bug 29431260.	10/10/2016	9.3	CVE-2016-3900
google -- android	Multiple integer overflows in drivers/crypto/msm/qcedev.c in the Qualcomm cryptographic engine driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29999161 and Qualcomm internal bug CR 1046434.	10/10/2016	9.3	CVE-2016-3901
google -- android	drivers/media/platform/msm/camera_v2/sensor/csid/msm_csid.c in the Qualcomm camera driver in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29513227 and Qualcomm internal bug CR 1040857.	10/10/2016	9.3	CVE-2016-3903
google -- android	CORE/HDD/src/wlan_hdd_main.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application that sends a SENDACTIONFRAME command, aka Android internal bug 28061823 and Qualcomm internal bug CR 1001449.	10/10/2016	9.3	CVE-2016-3905
google -- android	The SoftMPEG4 component 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, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30033990.	10/10/2016	9.3	CVE-2016-3909
google -- android	services/soundtrigger/SoundTriggerHwService.cpp in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30148546.	10/10/2016	9.3	CVE-2016-3910
google -- android	core/java/android/os/Process.java in Zygote in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30143607.	10/10/2016	9.3	CVE-2016-3911

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	The framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allow attackers to gain privileges via a crafted application, aka internal bug 30202481.	10/10/2016	9.3	CVE-2016-3912
google -- android	media/libmediaplayerservice/MediaPlayerService.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, 6.x before 2016-10-01, and 7.0 before 2016-10-01 does not validate a certain static_cast operation, which allows attackers to gain privileges via a crafted application, aka internal bug 30204103.	10/10/2016	9.3	CVE-2016-3913
google -- android	Race condition in providers/telephony/MmsProvider.java in Telephony in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application that modifies a database between two open operations, aka internal bug 30481342.	10/10/2016	9.3	CVE-2016-3914
google -- android	camera/src/camera_metadata.c in the Camera service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30591838.	10/10/2016	9.3	CVE-2016-3915
google -- android	camera/src/camera_metadata.c in the Camera service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 30741779.	10/10/2016	9.3	CVE-2016-3916
google -- android	The fingerprint login feature in Android 6.0.1 before 2016-10-01 and 7.0 before 2016-10-01 does not track the user account during the authentication process, which allows physically proximate attackers to authenticate as an arbitrary user by leveraging lockscreen access, aka internal bug 30744668.	10/10/2016	7.2	CVE-2016-3917
google -- android	id3/ID3.cpp in libstagefright in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 30744884.	10/10/2016	7.1	CVE-2016-3920
google -- android	libsysutils/src/FrameworkListener.cpp in Framework Listener in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 29831647.	10/10/2016	9.3	CVE-2016-3921
google -- android	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5, 5X, 6, and 6P devices has unknown impact and attack vectors, aka internal bug 28823953.	10/10/2016	10.0	CVE-2016-3926
google -- android	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5X and 6P devices has unknown impact and attack vectors, aka internal bug 28823244.	10/10/2016	10.0	CVE-2016-3927
google -- android	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30019362 and MediaTek internal bug ALPS02829384.	10/10/2016	9.3	CVE-2016-3928
google -- android	Unspecified vulnerability in a Qualcomm component in Android before 2016-10-05 on Nexus 5X and 6P devices has unknown impact and attack vectors, aka internal bug 28823675.	10/10/2016	10.0	CVE-2016-3929
google -- android	The NVIDIA MMC test driver in Android before 2016-10-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28760138.	10/10/2016	9.3	CVE-2016-3930
google -- android	drivers/misc/qseecom.c in the Qualcomm QSEE Communicator driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29157595 and Qualcomm internal bug CR 1036418.	10/10/2016	9.3	CVE-2016-3931
google -- android	mediaserver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 29161895 and MediaTek internal bug ALPS02770870.	10/10/2016	9.3	CVE-2016-3932
google -- android	mediaserver in Android before 2016-10-05 on Nexus 9 and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 29421408.	10/10/2016	9.3	CVE-2016-3933
google -- android	drivers/media/platform/msm/camera_v2/sensor/io/msm_camera_cci_i2c.c in the Qualcomm camera driver in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices relies on variable-length arrays, which allows attackers to gain privileges via a crafted application, aka Android internal bug 30102557 and Qualcomm internal bug CR 789704.	10/10/2016	9.3	CVE-2016-3934
google -- android	Multiple integer overflows in drivers/crypto/msm/qcedev.c in the Qualcomm cryptographic engine driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29999665 and Qualcomm internal bug CR 1046507.	10/10/2016	9.3	CVE-2016-3935
google -- android	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30019037 and MediaTek internal bug ALPS02829568.	10/10/2016	9.3	CVE-2016-3936
google -- android	The MediaTek video driver in Android before 2016-10-05 allows attackers to gain privileges via a crafted application, aka Android internal bug 30030994 and MediaTek internal bug ALPS02834874.	10/10/2016	9.3	CVE-2016-3937
google -- android	drivers/video/msm/mdss/mdss_mdp_overlay.c in the Qualcomm video driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 30019716 and Qualcomm internal bug CR 1049232.	10/10/2016	9.3	CVE-2016-3938
google -- android	drivers/video/msm/mdss/mdss_debug.c in the Qualcomm video driver in Android before 2016-10-05 on Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 30874196 and Qualcomm internal bug CR 1001224.	10/10/2016	9.3	CVE-2016-3939
google -- android	The Synaptics touchscreen driver in Android before 2016-10-05 on Nexus 6P and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 30141991.	10/10/2016	9.3	CVE-2016-3940
google -- android	The GPS component in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows man-in-the-middle attackers to cause a denial of service (memory consumption, and device hang or reboot) via a large xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 29555864.	10/10/2016	7.1	CVE-2016-5348
google -- android	The Synaptics touchscreen driver in Android before 2016-10-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application, aka internal bug 30537088.	10/10/2016	9.3	CVE-2016-6672
google -- android	The NVIDIA camera driver in Android before 2016-10-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 30204201.	10/10/2016	9.3	CVE-2016-6673
google -- android	Off-by-one error in CORE/HDD/src/wlan_hdd_hostapd.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X and Android One devices allows attackers to gain privileges or cause a denial of service (buffer overflow) via a crafted application that makes a linkspeed ioctl call, aka Android internal bug 30873776 and Qualcomm internal bug CR 1000861.	10/10/2016	9.3	CVE-2016-6675
google -- android	Off-by-one error in CORE/HDD/src/wlan_hdd_cfg.c in the Qualcomm Wi-Fi driver in Android before 2016-10-05 on Nexus 5X and Android One devices allows attackers to gain privileges or cause a denial of service (buffer overflow) via a crafted application that makes a GET_CFG ioctl call, aka Android internal bug 30874066 and Qualcomm internal bug CR 1000853.	10/10/2016	9.3	CVE-2016-6676
google -- android	The sound driver in the kernel in Android before 2016-10-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Nexus Player devices allows attackers to cause a denial of service (reboot) via a crafted application, aka internal bug 28838221.	10/10/2016	7.1	CVE-2016-6690
google -- android	service/jni/com_android_server_wifi_Gbk2Utf.cpp in the Qualcomm Wi-Fi gbk2utf module in Android before 2016-10-05 allows remote attackers to cause a denial of service (framework crash) or possibly have unspecified other impact via an access point that has a malformed SSID with GBK encoding, aka Qualcomm internal bug CR 978452.	10/10/2016	7.5	CVE-2016-6691
google -- android	drivers/video/msm/mdss/mdss_mdp_pp.c in the Qualcomm MDSS driver in Android before 2016-10-05 allows attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via unknown vectors, aka Qualcomm internal bug CR 1004933.	10/10/2016	7.5	CVE-2016-6692
google -- android	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via an invalid data length, aka Qualcomm internal bug CR 1027585.	10/10/2016	7.5	CVE-2016-6693
google -- android	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via crafted parameter data, aka Qualcomm internal bug CR 1033525.	10/10/2016	7.5	CVE-2016-6694
google -- android	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted visualizer data length, aka Qualcomm internal bug CR 1033540.	10/10/2016	7.5	CVE-2016-6695
google -- android	sound/soc/msm/qdsp6v2/msm-ds2-dap-config.c in a Qualcomm QDSP6v2 driver in Android before 2016-10-05 allows attackers to cause a denial of service or possibly have unspecified other impact via a large negative value for the data length, aka Qualcomm internal bug CR 1041130.	10/10/2016	7.5	CVE-2016-6696
intel -- solid-state_drive_toolbox	The updater subsystem in Intel SSD Toolbox before 3.3.7 allows local users to gain privileges via unspecified vectors.	10/10/2016	7.2	CVE-2016-8101
linux -- linux_kernel	Multiple race conditions in drivers/char/adsprpc.c and drivers/char/adsprpc_compat.c in the ADSPRPC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (zero-value write) or possibly have unspecified other impact via a COMPAT_FASTRPC_IOCTL_INVOKE_FD ioctl call.	10/10/2016	7.5	CVE-2015-0572
linux -- linux_kernel	drivers/soc/qcom/qdsp6v2/voice_svc.c in the QDSP6v2 Voice Service driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write request, as demonstrated by a voice_svc_send_req buffer overflow.	10/10/2016	7.5	CVE-2016-5343
ruckus -- wireless_h500	Ruckus Wireless H500 web management interface authenticated command injection	10/10/2016	9.0	CVE-2016-1000216
haxx -- libcurl	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.	07/10/2016	7.5	CVE-2016-7167
mirror_manager_project -- mirror_manager	Mirror Manager version 0.7.2 and older is vulnerable to remote code execution in the checkin code	07/10/2016	7.5	CVE-2016-1000003
openstack -- cinder	The image parser in OpenStack Cinder 7.0.2 and 8.0.0 through 8.1.1; Glance before 11.0.1 and 12.0.0; and Nova before 12.0.4 and 13.0.0 does not properly limit qemu-img calls, which might allow attackers to cause a denial of service (memory and disk consumption) via a crafted disk image.	07/10/2016	7.8	CVE-2015-5162
redhat -- cloudforms_management_engine	Red Hat CloudForms Management Engine 4.1 does not properly handle regular expressions passed to the expression engine via the JSON API and the web-based UI, which allows remote authenticated users to execute arbitrary shell commands by leveraging the ability to view and filter collections.	07/10/2016	9.0	CVE-2016-7040

Semana 03/10/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- nx-os	Cisco NX-OS 4.1 through 7.3 and 11.0 through 11.2 on Nexus 2000, 3000, 3500, 5000, 5500, 5600, 6000, 7000, 7700, and 9000 devices allows remote attackers to cause a denial of service (device crash) via malformed IPv4 DHCP packets to the DHCPv4 relay agent, aka Bug IDs CSCuq39250, CSCus21733, CSCus21739, CSCut76171, and CSCux67182.	06/10/2016	7.8	CVE-2015-6393
cisco -- nx-os	Buffer overflow in the Overlay Transport Virtualization (OTV) GRE feature in Cisco NX-OS 5.0 through 7.3 on Nexus 7000 and 7700 devices allows remote attackers to execute arbitrary code via long parameters in a packet header, aka Bug ID CSCuy95701.	06/10/2016	10.0	CVE-2016-1453
cisco -- ios_xr	Cisco IOS XR 6.1.1 allows local users to execute arbitrary OS commands as root by leveraging admin privileges, aka Bug ID CSCva38349.	06/10/2016	7.2	CVE-2016-6428
cisco -- firepower_management_center	The Threat Management Console in Cisco Firepower Management Center 5.2.0 through 6.0.1 allows remote authenticated users to execute arbitrary commands via crafted web-application parameters, aka Bug ID CSCva30872.	06/10/2016	9.0	CVE-2016-6433
contus-video-comments_project -- contus-video-comments	Unauthenticated remote .jpg file upload in contus-video-comments v1.0 wordpress plugin	06/10/2016	9.4	CVE-2016-1000112
dukapress_project -- dukapress	Blind SQL Injection in wordpress plugin dukapress v2.5.9	06/10/2016	7.5	CVE-2015-1000011
huge-it -- huge-it_image_gallery	XSS and SQLi in huge IT gallery v1.1.5 for Joomla	06/10/2016	7.5	CVE-2016-1000113
huge-it -- video_gallery	Unauthenticated SQL Injection in Huge-IT Video Gallery v1.0.9 for Joomla	06/10/2016	7.5	CVE-2016-1000123
huge-it -- portfolio_gallery	Unauthenticated SQL Injection in Huge-IT Portfolio Gallery Plugin v1.0.6	06/10/2016	7.5	CVE-2016-1000124
huge-it -- huge-it_catalog	Unauthenticated SQL Injection in Huge-IT Catalog v1.0.7 for Joomla	06/10/2016	7.5	CVE-2016-1000125
zotpress_project -- zotpress	Zotpress plugin for WordPress SQLi in zp_get_account()	06/10/2016	7.5	CVE-2016-1000217
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.	05/10/2016	10.0	CVE-2016-7020
american_auto-matrix -- aspect-matrix_building_automation_front-end_solutions_application	American Auto-Matrix Aspect-Nexus Building Automation Front-End Solutions application before 3.0.0 and Aspect-Matrix Building Automation Front-End Solutions application store passwords in cleartext, which allows remote attackers to obtain sensitive information by reading a file.	05/10/2016	7.5	CVE-2016-2308
animas -- onetouch_ping_firmware	Johnson & Johnson Animas OneTouch Ping devices do not properly generate random numbers, which makes it easier for remote attackers to spoof meters by sniffing the network and then engaging in an authentication handshake.	05/10/2016	7.8	CVE-2016-5085
animas -- onetouch_ping_firmware	Johnson & Johnson Animas OneTouch Ping devices allow remote attackers to bypass authentication via replay attacks.	05/10/2016	9.3	CVE-2016-5086
animas -- onetouch_ping_firmware	Johnson & Johnson Animas OneTouch Ping devices mishandle acknowledgements, which makes it easier for remote attackers to bypass authentication via a custom communication protocol.	05/10/2016	9.3	CVE-2016-5686
beckhoff -- embedded_pc_images	Beckhoff Embedded PC images before 2014-10-22 and Automation Device Specification (ADS) TwinCAT components do not restrict the number of authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack.	05/10/2016	9.4	CVE-2014-5414
beckhoff -- embedded_pc_images	Beckhoff Embedded PC images before 2014-10-22 and Automation Device Specification (ADS) TwinCAT components might allow remote attackers to obtain access via the (1) Windows CE Remote Configuration Tool, (2) CE Remote Display service, or (3) TELNET service.	05/10/2016	9.4	CVE-2014-5415
cisco -- ios_xe	Cisco IOS XE 3.1 through 3.17 and 16.1 through 16.2 allows remote attackers to cause a denial of service (device reload) via crafted ICMP packets that require NAT, aka Bug ID CSCuw85853.	05/10/2016	7.8	CVE-2016-6378
cisco -- ios	Cisco IOS 12.2 and IOS XE 3.14 through 3.16 and 16.1 allow remote attackers to cause a denial of service (device reload) via crafted IP Detail Record (IPDR) packets, aka Bug ID CSCuu35089.	05/10/2016	7.8	CVE-2016-6379
cisco -- ios	The DNS forwarder in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.15 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (data corruption or device reload) via a crafted DNS response, aka Bug ID CSCup90532.	05/10/2016	8.3	CVE-2016-6380
cisco -- ios	Cisco IOS 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.18 and 16.1 allow remote attackers to cause a denial of service (memory consumption or device reload) via fragmented IKEv1 packets, aka Bug ID CSCuy47382.	05/10/2016	7.1	CVE-2016-6381
cisco -- ios	Cisco IOS 15.2 through 15.6 and IOS XE 3.6 through 3.17 and 16.1 allow remote attackers to cause a denial of service (device restart) via a malformed IPv6 Protocol Independent Multicast (PIM) register packet, aka Bug ID CSCuy16399.	05/10/2016	7.8	CVE-2016-6382
cisco -- ios	Cisco IOS 12.2 through 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.17 and 16.2 allow remote attackers to cause a denial of service (device reload) via crafted fields in an H.323 message, aka Bug ID CSCux04257.	05/10/2016	7.8	CVE-2016-6384
cisco -- ios	Memory leak in the Smart Install client implementation in Cisco IOS 12.2 and 15.0 through 15.2 and IOS XE 3.2 through 3.8 allows remote attackers to cause a denial of service (memory consumption) via crafted image-list parameters, aka Bug ID CSCuy82367.	05/10/2016	7.8	CVE-2016-6385
cisco -- ios_xe	Cisco IOS XE 3.1 through 3.17 and 16.1 on 64-bit platforms allows remote attackers to cause a denial of service (data-structure corruption and device reload) via fragmented IPv4 packets, aka Bug ID CSCux66005.	05/10/2016	7.8	CVE-2016-6386
cisco -- ios	Cisco IOS 12.2 and 15.0 through 15.3 allows remote attackers to cause a denial of service (traffic-processing outage) via a crafted series of Common Industrial Protocol (CIP) requests, aka Bug ID CSCur69036.	05/10/2016	7.8	CVE-2016-6391
cisco -- ios	Cisco IOS 12.2 and 15.0 through 15.3 and IOS XE 3.1 through 3.9 allow remote attackers to cause a denial of service (device restart) via a crafted IPv4 Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message, aka Bug ID CSCud36767.	05/10/2016	7.8	CVE-2016-6392
cisco -- ios	The AAA service in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.1 through 3.18 and 16.2 allows remote attackers to cause a denial of service (device reload) via a failed SSH connection attempt that is mishandled during generation of an error-log message, aka Bug ID CSCuy87667.	05/10/2016	7.1	CVE-2016-6393
f5 -- big-ip_local_traffic_manager	F5 BIG-IP LTM systems 11.x before 11.2.1 HF16, 11.3.x, 11.4.x before 11.4.1 HF11, 11.5.0, 11.5.1 before HF11, 11.5.2, 11.5.3, 11.5.4 before HF2, 11.6.0 before HF8, 11.6.1 before HF1, 12.0.0 before HF4, and 12.1.0 before HF2 allow remote attackers to modify or extract system configuration files via vectors involving NAT64.	05/10/2016	10.0	CVE-2016-5745
fortinet -- fortiwlc	The rsyncd server in Fortinet FortiWLC 6.1-2-29 and earlier, 7.0-9-1, 7.0-10-0, 8.0-5-0, 8.1-2-0, and 8.2-4-0 has a hardcoded rsync account, which allows remote attackers to read or write to arbitrary files via unspecified vectors.	05/10/2016	10.0	CVE-2016-7560
qemu -- qemu	Heap-based buffer overflow in the .receive callback of xlnx.xps-ethernetlite in QEMU (aka Quick Emulator) allows attackers to execute arbitrary code on the QEMU host via a large ethlite packet.	05/10/2016	10.0	CVE-2016-7161
sap -- netweaver	The (1) SCTC_REFRESH_EXPORT_TAB_COMP, (2) SCTC_REFRESH_CHECK_ENV, and (3) SCTC_TMS_MAINTAIN_ALOG functions in the SCTC subpackage in SAP Netweaver 7.40 SP 12 allow remote authenticated users with certain permissions to execute arbitrary commands via vectors involving a CALL 'SYSTEM' statement, aka SAP Security Note 2260344.	05/10/2016	9.0	CVE-2016-7435
emc -- networker_module_for_microsoft_applications	The client in EMC Replication Manager (RM) before 5.5.3.0_01-PatchHotfix, EMC Network Module for Microsoft 3.x, and EMC Networker Module for Microsoft 8.2.x before 8.2.3.6 allows remote RM servers to execute arbitrary commands by placing a crafted script in an SMB share.	04/10/2016	7.5	CVE-2016-0913
emc -- solutions_enabler	The vApp Managers web application in EMC Unisphere for VMAX Virtual Appliance 8.x before 8.3.0 and Solutions Enabler Virtual Appliance 8.x before 8.3.0 allows remote authenticated users to execute arbitrary code via crafted input to the (1) GeneralCmdRequest, (2) PersistantDataRequest, or (3) GetCommandExecRequest class.	04/10/2016	9.0	CVE-2016-6645
emc -- solutions_enabler	The vApp Managers web application in EMC Unisphere for VMAX Virtual Appliance 8.x before 8.3.0 and Solutions Enabler Virtual Appliance 8.x before 8.3.0 allows remote attackers to execute arbitrary code via crafted input to the (1) GetSymmCmdRequest or (2) RemoteServiceHandler class.	04/10/2016	10.0	CVE-2016-6646
adodb_project -- adodb	The qstr method in the PDO driver in the ADOdb Library for PHP before 5.x before 5.20.7 might allow remote attackers to conduct SQL injection attacks via vectors related to incorrect quoting.	03/10/2016	7.5	CVE-2016-7405
apache -- tomcat	The Tomcat init script in the tomcat7 package before 7.0.56-3+deb8u4 and tomcat8 package before 8.0.14-1+deb8u3 on Debian jessie and the tomcat6 and libtomcat6-java packages before 6.0.35-1ubuntu3.8 on Ubuntu 12.04 LTS, the tomcat7 and libtomcat7-java packages before 7.0.52-1ubuntu0.7 on Ubuntu 14.04 LTS, and tomcat8 and libtomcat8-java packages before 8.0.32-1ubuntu1.2 on Ubuntu 16.04 LTS allows local users with access to the tomcat account to gain root privileges via a symlink attack on the Catalina log file, as demonstrated by /var/log/tomcat7/catalina.out.	03/10/2016	7.2	CVE-2016-1240
apache -- struts	Apache Struts 2 before 2.3.29 and 2.5.x before 2.5.1 allow attackers to have unspecified impact via vectors related to improper action name clean up.	03/10/2016	7.5	CVE-2016-4436
apache -- myfaces	CoreResponseStateManager in Apache MyFaces Trinidad 1.0.0 through 1.0.13, 1.2.x before 1.2.15, 2.0.x before 2.0.2, and 2.1.x before 2.1.2 might allow attackers to conduct deserialization attacks via a crafted serialized view state string.	03/10/2016	7.5	CVE-2016-5019
c-ares_project -- c-ares	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly execute arbitrary code via a hostname with an escaped trailing dot.	03/10/2016	7.5	CVE-2016-5180
f5 -- big-ip_access_policy_manager	Virtual servers in F5 BIG-IP systems 11.5.0, 11.5.1 before HF11, 11.5.2, 11.5.3, 11.5.4 before HF2, 11.6.0 before HF8, 11.6.1 before HF1, 12.0.0 before HF4, and 12.1.0 before HF2, when configured with the HTTP Explicit Proxy functionality or SOCKS profile, allow remote attackers to modify the system configuration, read system files, and possibly execute arbitrary code via unspecified vectors.	03/10/2016	9.3	CVE-2016-5700
huawei -- usg2100	Buffer overflow in the Point-to-Point Protocol over Ethernet (PPPoE) module in Huawei USG2100, USG2200, USG5100, and USG5500 unified security gateways with software before V300R001C10SPC600, when CHAP authentication is configured on the server, allows remote attackers to cause a denial of service (server restart) or execute arbitrary code via crafted packets sent during authentication.	03/10/2016	9.3	CVE-2016-8276
huawei -- usg9520	Huawei USG9520, USG9560, and USG9580 unified security gateways with software before V300R001C01SPCa00 allow remote attackers to cause a denial of service (device restart) via an unspecified URL.	03/10/2016	7.8	CVE-2016-8278
redhat -- jboss_enterprise_application_platform	Red Hat JBoss Enterprise Application Platform (EAP) 7, when operating as a reverse-proxy with default buffer sizes, allows remote attackers to cause a denial of service (CPU and disk consumption) via a long URL.	03/10/2016	7.1	CVE-2016-7046
unadf_project -- unadf	Stack-based buffer overflow in the extractTree function in unADF allows remote attackers to execute arbitrary code via a long pathname.	03/10/2016	7.5	CVE-2016-1243
unadf_project -- unadf	The extractTree function in unADF allows remote attackers to execute arbitrary code via shell metacharacters in a directory name in an adf file.	03/10/2016	9.3	CVE-2016-1244