Vulnerability Summary for the Week of April 3, 2017

Please Note:

- The vulnerabilities are cattegorized by their level of severity which is either High, Medium or Low.
- The CVE indentity number is the publicly known ID given to that particular vulnerability. Therefore you can search the status of that particular vulnerability using that ID.
- The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- acrobat_reader	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the rendering engine. Successful exploitation could lead to arbitrary code execution.	2017-03-31	10.0	CVE-2017-3010 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2398 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service	2017-04-01	9.3	CVE-2017-2401 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

	(memory corruption) via a crafted app.			CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. The issue involves the "Security" component. It allows remote attackers to bypass intended access restrictions by leveraging a successful result from a SecKeyRawVerify API call with an empty signature.	2017-04-01	7.5	CVE-2017-2423 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves nghttp2 before 1.17.0 in the "HTTPProtocol" component. It allows remote HTTP/2 servers to have an unspecified impact via unknown vectors.	2017-04-01	7.5	CVE-2017-2428 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "HomeKit" component. It allows attackers to have an unspecified impact by leveraging the presence of Home Control on Control Center.	2017-04-01	10.0	CVE-2017-2434 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (integer overflow) via a crafted app.	2017-04-01	9.3	CVE-2017-2440 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The	2017-04-01	9.3	CVE-2017-2441 BID (link is external) CONFIRM (link is external) CONFIRM (link

	issue involves the "libc++abi" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code via a crafted C++ app that is mishandled during demangling.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Security" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (buffer overflow) via a crafted app.	2017-04-01	9.3	CVE-2017-2451 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	7.6	CVE-2017-2456 BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Keyboards" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2458 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app.	2017-04-01	9.3	CVE-2017-2472 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2473 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. An off-by-one error allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2474 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	7.6	CVE-2017-2478 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2482 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A buffer	2017-04-01	9.3	CVE-2017-2483 BID (link is external) CONFIRM (link is external) CONFIRM (link

	overflow allows attackers to execute arbitrary code in a privileged context via a crafted app.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Security" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted X.509 certificate file.	2017-04-01	9.3	CVE-2017-2485 BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2490 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves mishandling of profile uninstall actions in the "MCX Client" component when a profile has multiple payloads. It allows remote attackers to bypass intended access restrictions by leveraging Active Directory certificate trust that should not have remained.	2017-04-01	7.5	CVE-2017-2402 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOATAFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2408 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The	2017-04-01	9.3	CVE-2017-2410 BID (link is external)

	issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app.			CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2420 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleGraphicsPowerManagement" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2421 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Multi-Touch" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2422 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2427 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireAVC" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2436 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireAVC" component. It allows local users to gain privileges or cause a	2017-04-01	7.2	CVE-2017-2437 BID (link is external) CONFIRM (link is external)

	denial of service (memory corruption) via unspecified vectors.			
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleRAID" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app.	2017-04-01	9.3	CVE-2017-2438 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2443 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app.	2017-04-01	9.3	CVE-2017-2449 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "libxslt" component. It allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.	2017-04-01	7.5	CVE-2017-2477 BID (link is external) CONFIRM (link is external)
huawei -- campus_s9700_firmware	Huawei Campus S7700 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300; S9300 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300; S9700 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300 allow unauthorized users to upgrade the bootrom or bootload software, bypass a Menu protection mechanism, conduct a Menu compromise attack, or bypass a Menu/upgrade protection mechanism.	2017-04-02	7.5	CVE-2014-4707 CONFIRM (link is external)

huawei -- cloudengine_5800_firmware	Huawei CloudEngine 12800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 5800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 6800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 7800 with software V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 8800 with software V100R006C00; and Secospace USG6600 with software V500R001C00 allow remote unauthenticated attackers to craft specific IPFPM packets to trigger an integer overflow and cause the device to reset.	2017-04-02	7.1	CVE-2016-8795 CONFIRM (link is external) BID (link is external)
huawei -- fusionaccess	Huawei FusionAccess with software V100R005C10,V100R005C20 could allow attackers to craft and send a malformed HDP protocol packet to cause the virtual cloud desktop to be displaying an error and not usable.	2017-04-02	7.8	CVE-2015-7844 CONFIRM (link is external)
huawei -- hisuite	Huawei PC client software HiSuite 4.0.5.300_OVE has a dynamic link library (DLL) hijack vulnerability; an attacker can make the system load malicious DLL files to execute arbitrary code.	2017-04-02	7.2	CVE-2016-8274 CONFIRM (link is external)
huawei -- mate_8_firmware	ION memory management module in Huawei Mate 8 phones with software NXT-AL10C00B197 and earlier versions, NXT-DL10C00B197 and earlier versions, NXT-TL10C00B197 and earlier versions, NXT-CL10C00B197 and earlier versions allows attackers to cause a denial of service (restart).	2017-04-02	7.1	CVE-2016-8756 CONFIRM (link is external) BID (link is external)
huawei -- mate_8_firmware	ION memory management module in Huawei Mate8 phones with software NXT-AL10C00B561 and earlier versions, NXT-CL10C00B561 and earlier versions, NXT-DL10C00B561 and earlier versions, NXT-TL10C00B561 and earlier versions allows attackers to cause a denial of service	2017-04-02	7.1	CVE-2016-8758 CONFIRM (link is external) BID (link is external)

	(restart).			
huawei -- nem-al10_firmware	Touch Panel (TP) driver in Huawei NEM phones with software Versions before NEM-AL10C00B130, Versions before NEM-UL10C17B160, Versions before NEM-UL10C00B160, Versions before NEM-TL00C01B160 allows attackers to get root privilege or crash the system or execute arbitrary code, related to a buffer overflow.	2017-04-02	7.2	CVE-2016-8775 CONFIRM (link is external) BID (link is external)
huawei -- oceanstor_5600_v3_firmware	Huawei OceanStor 5600 V3 with V300R003C00C10 and earlier versions allows attackers with administrator privilege to inject a command into a specific command's parameters, and run this injected command with root privilege.	2017-04-02	9.0	CVE-2016-8801 CONFIRM (link is external) BID (link is external)
huawei -- p8_lite_firmware	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an improper resource release vulnerability, which allows attackers to cause a system restart or privilege elevation.	2017-04-02	9.3	CVE-2016-8763 CONFIRM (link is external) BID (link is external)
huawei -- p9_plus_firmware	Video driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and Huawei Honor 6 phones with software versions before H60-L02_6.10.1 has a stack overflow vulnerability, which allows attackers to crash the system or escalate user privilege.	2017-04-02	9.3	CVE-2016-8759 CONFIRM (link is external) BID (link is external)
huawei -- p9_plus_firmware	Touchscreen driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and Huawei Honor 6 phones with software versions before H60-L02_6.10.1 has a heap overflow vulnerability, which allows attackers to crash the system or escalate user privilege.	2017-04-02	9.3	CVE-2016-8760 CONFIRM (link is external) BID (link is external)
huawei -- p9_plus_firmware	Video driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and Huawei Honor 6 phones with software versions before	2017-04-02	9.3	CVE-2016-8761 CONFIRM (link is external) BID (link is

	H60-L02_6.10.1 has a stack overflow vulnerability, which allows attackers to crash the system or escalate user privilege.			external)
huawei -- quidway_s6700_firmware	Huawei Quidway S9700 V200R003C00SPC500, Quidway S9300 V200R003C00SPC500, Quidway S7700 V200R003C00SPC500, Quidway S6700 V200R003C00SPC300, Quidway S6300 V200R003C00SPC300, Quidway S5700 V200R003C00SPC300, Quidway S5300 V200R003C00SPC300 enable attackers to launch DoS attacks by crafting and sending malformed packets to these vulnerable products.	2017-04-02	7.8	CVE-2014-3224 CONFIRM (link is external)
huawei -- s2750_firmware	Huawei Campus S3700HI with software V200R001C00SPC300; Campus S5700 with software V200R002C00SPC100; Campus S7700 with software V200R003C00SPC300,V200R003C00SPC500; LSW S9700 with software V200R001C00SPC300,V200R003C00SPC300,V200R003C00SPC500; S2350 with software V200R003C00SPC300; S2750 with software V200R003C00SPC300; S5300 with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S5700 with software V200R001C00SPC300,V200R003C00SPC300; S6300 with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S6700 S3300HI with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S7700 with software V200R001C00SPC300; S9300 with software V200R001C00SPC300,V200R003C00SPC300,V200R003C00SPC500; S9300E with software V200R003C00SPC300,V200R003C00SPC500 allow attackers to keep sending malformed packets to cause a denial of service (DoS) attack, aka a heap overflow.	2017-04-02	7.8	CVE-2014-4706 CONFIRM (link is external)
huawei -- s6300_firmware	Huawei S9300 with software before V100R006SPH013 and S2300,S3300,S5300,S6300	2017-04-02	7.8	CVE-2014-3223 CONFIRM (link is external)

	with software before V100R006SPH010 support Y.1731 and therefore have the Y.1731 vulnerability in processing special packets. The vulnerability causes the restart of switches.			
huawei -- tecal_bh621_v2_firmware	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier	2017-04-02	7.5	CVE-2014-9693 CONFIRM (link is external)

	versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions could allow attackers to execute arbitrary code or restart the system via crafted DNS packets.			
huawei -- usg5500_firmware	Huawei USG5500 with software V300R001C00 and V300R001C00 allows attackers to bypass the anti-DDoS module of the USGs to cause a denial of service condition on the backend server.	2017-04-02	7.8	CVE-2016-8798 CONFIRM (link is external) BID (link is external)
huawei -- usg9580_firmware	Huawei USG9520 V300R001C01, USG9560 V300R001C01, and USG9580 V300R001C01 allow unauthenticated attackers to send abnormal DHCP request packets to the affected products to trigger a DoS condition.	2017-04-02	7.8	CVE-2016-8796 CONFIRM (link is external) BID (link is external)
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0 and 7.0 are vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 2000833.	2017-03-31	8.5	CVE-2016-6111 CONFIRM (link is external) BID (link is external)
ibm -- rational_software_architect_design_manager	IBM Jazz Foundation is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 2000784.	2017-03-31	7.5	CVE-2016-9707 BID (link is external) CONFIRM (link is external)
illumos -- illumos	illumos osnet-incorporation bcopy() and bzero() implementations make signed instead of unsigned comparisons allowing a system crash.	2017-03-31	7.8	CVE-2016-6560 CONFIRM (link is external) CONFIRM CONFIRM
illumos -- illumos	illumos smbsrv NULL pointer dereference allows system crash.	2017-03-31	7.8	CVE-2016-6561 CONFIRM (link is external)

				CONFIRM CONFIRM
linux -- linux_kernel	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for a certain match field, related to the keyring_search_iterator function in keyring.c.	2017-03-31	7.2	CVE-2017-2647 CONFIRM BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	Use-after-free vulnerability in fs/crypto/ in the Linux kernel before 4.10.7 allows local users to cause a denial of service (NULL pointer dereference) or possibly gain privileges by revoking keyring keys being used for ext4, f2fs, or ubifs encryption, causing cryptographic transform objects to be freed prematurely.	2017-03-31	7.2	CVE-2017-7374 CONFIRM BID (link is external) CONFIRM (link is external) CONFIRM
multi-router_looking_glass_project -- multi-router_looking_glass	fastping.c in MRLG (aka Multi-Router Looking Glass) before 5.5.0 allows remote attackers to cause an arbitrary memory write and memory corruption.	2017-03-31	7.5	CVE-2014-3931 CONFIRM (link is external) MISC (link is external) MISC (link is external)
opensuse_project -- opensuse	Blkid in util-linux before 2.26rc-1 allows local users to execute arbitrary code.	2017-03-31	7.2	CVE-2014-9114 FEDORA FEDORA SUSE MLIST (link is external) BID (link is external) XF (link is external) CONFIRM (link is external) CONFIRM (link is external) GENTOO
snoopy -- snoopy	The _httpsrequest function in Snoopy allows remote attackers to execute arbitrary commands. NOTE: this issue exists dues to an incomplete fix for CVE-2008-4796.	2017-03-31	7.5	CVE-2008-7313 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external)

				BID (link is external) CONFIRM (link is external) XF (link is external) REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) GENTOO MISC (link is external)
snoopy -- snoopy	Snoopy allows remote attackers to execute arbitrary commands.	2017-03-31	7.5	CVE-2014-5008 REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) CONFIRM (link is external) DEBIAN MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC (link is external)
snoopy -- snoopy	Snoopy allows remote attackers to execute arbitrary commands. NOTE: this vulnerability exists due to an incomplete fix for CVE-2014-5008.	2017-03-31	7.5	CVE-2014-5009 REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) REDHAT (link is external) CONFIRM (link

				is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) XF (link is external) CONFIRM (link is external) MISC (link is external) MISC (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- acrobat_reader	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable buffer overflow vulnerability in the JPEG2000 parser. Successful exploitation could lead to information disclosure.	2017-03-31	5.0	CVE-2017-3009 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Carbon" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted .dfont file.	2017-04-01	6.8	CVE-2017-2379 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products.	2017-04-01	5.0	CVE-2017-2380

	iOS before 10.3 is affected. The issue involves the Simple Certificate Enrollment Protocol (SCEP) implementation in the the "Profiles" component. It allows remote attackers to bypass cryptographic protection mechanisms by leveraging DES support.			BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Safari Reader" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site.	2017-04-01	4.3	CVE-2017-2393 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "SafariViewController" component. It allows attackers to obtain sensitive information by leveraging the SafariViewController's incorrect synchronization of Safari cache clearing.	2017-04-01	5.0	CVE-2017-2400 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Quick Look" component. It allows remote attackers to trigger telephone calls to arbitrary numbers via a tel: URL in a PDF document, as exploited in the wild in October 2016.	2017-04-01	5.0	CVE-2017-2404 BID (link is external) CONFIRM (link is external) MISC (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file.	2017-04-01	6.8	CVE-2017-2406 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file.	2017-04-01	6.8	CVE-2017-2407 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link

				is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "iTunes Store" component. It allows man-in-the-middle attackers to modify the client-server data stream to iTunes sandbox web services by leveraging use of cleartext HTTP.	2017-04-01	4.3	CVE-2017-2412 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "DataAccess" component. It allows remote attackers to access Exchange traffic in opportunistic circumstances by leveraging a mistake in typing an e-mail address.	2017-04-01	5.0	CVE-2017-2414 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code by leveraging an unspecified "type confusion."	2017-04-01	6.8	CVE-2017-2415 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted image file.	2017-04-01	6.8	CVE-2017-2416 BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreGraphics" component. It allows remote attackers to cause a denial of service (infinite recursion) via a crafted image.	2017-04-01	4.3	CVE-2017-2417 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

				CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Audio" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file.	2017-04-01	6.8	CVE-2017-2430 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted JPEG file.	2017-04-01	6.8	CVE-2017-2432 BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file.	2017-04-01	6.8	CVE-2017-2435 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted font file.	2017-04-01	5.8	CVE-2017-2439 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products.	2017-04-01	4.3	CVE-2017-2448 BID (link is

	iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. The issue involves the "Keychain" component. It allows man-in-the-middle attackers to bypass an iCloud Keychain secret protection mechanism by leveraging lack of authentication for OTR packets.			external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted font file.	2017-04-01	5.8	CVE-2017-2450 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to cause a denial of service (resource consumption) via a crafted text message.	2017-04-01	5.0	CVE-2017-2461 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Audio" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file.	2017-04-01	6.8	CVE-2017-2462 BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service	2017-04-01	6.8	CVE-2017-2467 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	(memory corruption and application crash) via a crafted file.			CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Phone" component. It allows attackers to trigger telephone calls to arbitrary numbers via a third-party app.	2017-04-01	5.0	CVE-2017-2484 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file.	2017-04-01	6.8	CVE-2017-2487 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- keynote	An issue was discovered in certain Apple products. Pages before 6.1, Numbers before 4.1, and Keynote before 7.1 on macOS and Pages before 3.1, Numbers before 3.1, and Keynote before 3.1 on iOS are affected. The issue involves the "Export" component. It allows users to bypass iWork PDF password protection by leveraging use of 40-bit RC4.	2017-04-01	5.0	CVE-2017-2391 BID (link is external) CONFIRM (link is external)
apple -- mac_os_server	An issue was discovered in certain Apple products. macOS Server before 5.3 is affected. The issue involves the "Wiki Server" component. It allows remote attackers to enumerate user accounts via unspecified vectors.	2017-04-01	5.0	CVE-2017-2382 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "sudo" component. It allows remote authenticated users to gain privileges by leveraging membership in the admin group on a network directory server.	2017-04-01	6.5	CVE-2017-2381 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves	2017-04-01	4.3	CVE-2017-2388 BID (link is external)

	the "IOFireWireFamily" component. It allows attackers to cause a denial of service (NULL pointer dereference) via a crafted app.			CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Printing" component. A format-string vulnerability allows remote attackers to execute arbitrary code via a crafted ipp: or ipps: URL.	2017-04-01	6.8	CVE-2017-2403 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Menus" component. It allows attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted app.	2017-04-01	5.8	CVE-2017-2409 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "QuickTime" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted media file.	2017-04-01	6.8	CVE-2017-2413 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "SecurityFoundation" component. A double free vulnerability allows remote attackers to execute arbitrary code via a crafted certificate.	2017-04-01	6.8	CVE-2017-2425 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "iBooks" component. It allows remote attackers to obtain sensitive information from local files via a file: URL in an iBooks file.	2017-04-01	4.3	CVE-2017-2426 BID (link is external) MISC (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "FinderKit" component. It allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging unexpected permission changes during an iCloud Sharing Send Link action.	2017-04-01	5.0	CVE-2017-2429 BID (link is external) CONFIRM (link is external)

apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "CoreMedia" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted .mov file.	2017-04-01	6.8	CVE-2017-2431 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to obtain sensitive information from kernel memory via a crafted app.	2017-04-01	4.3	CVE-2017-2489 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the system-installation subsystem of the "System Integrity Protection" component. It allows attackers to modify the contents of a protected disk location via a crafted app.	2017-04-01	4.3	CVE-2017-6974 BID (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.	2017-04-01	4.3	CVE-2017-2367 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar by leveraging text input during the loading of a page.	2017-04-01	5.0	CVE-2017-2376 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows attackers to cause a denial of service (memory corruption and application crash) by leveraging a window-close action during a debugger-pause state.	2017-04-01	5.0	CVE-2017-2377 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products.	2017-04-01	6.8	CVE-2017-2378 BID (link is

	iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves bookmark creation in the "WebKit" component. It allows remote attackers to execute arbitrary code or spoof a bookmark by leveraging mishandling of links during drag-and-drop actions.			external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.	2017-04-01	4.3	CVE-2017-2386 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof an HTTP authentication sheet or cause a denial of service via a crafted web site.	2017-04-01	5.8	CVE-2017-2389 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	6.8	CVE-2017-2392 BID (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2394 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2395 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2396 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2405 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass a Content Security Policy protection mechanism via unspecified vectors.	2017-04-01	5.0	CVE-2017-2419 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves mishandling of OpenGL shaders in the "WebKit" component. It allows remote attackers to obtain sensitive information from process memory via a crafted web site.	2017-04-01	4.3	CVE-2017-2424 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2433 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit JavaScript Bindings" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive	2017-04-01	4.3	CVE-2017-2442 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	information via a crafted web site.			
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreGraphics" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2444 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted frame objects.	2017-04-01	4.3	CVE-2017-2445 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions.	2017-04-01	6.8	CVE-2017-2446 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted web site.	2017-04-01	5.8	CVE-2017-2447 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof FaceTime prompts in the user interface via a crafted web site.	2017-04-01	4.3	CVE-2017-2453 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is	2017-04-01	6.8	CVE-2017-2454 BID (link is external)

	affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2455 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2457 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2459 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2460 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the	2017-04-01	6.8	CVE-2017-2463 BID (link is external) MISC (link is external) CONFIRM (link is external)

	"WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2464 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2465 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2466 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2468 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote	2017-04-01	6.8	CVE-2017-2469 BID (link is external) CONFIRM (link is external) CONFIRM (link

	attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2470 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code via a crafted web site.	2017-04-01	6.8	CVE-2017-2471 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted use of frames on a web site.	2017-04-01	4.3	CVE-2017-2475 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2476 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive	2017-04-01	4.3	CVE-2017-2479 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link

	information via a crafted web site.			is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.	2017-04-01	4.3	CVE-2017-2480 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-04-01	6.8	CVE-2017-2481 BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to spoof the address bar via a crafted web site.	2017-04-01	4.3	CVE-2017-2486 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
getpixie -- pixie	Pixie 1.0.4 allows an admin/index.php s=login&m= XSS attack.	2017-03-31	4.3	CVE-2017-7359 MISC (link is external) BID (link is external) BID (link is external)
getpixie -- pixie	Pixie 1.0.4 allows an admin/index.php s=settings&x= XSS attack.	2017-03-31	4.3	CVE-2017-7360 MISC (link is external) BID (link is external)
getpixie -- pixie	Pixie 1.0.4 allows an admin/index.php s=publish&m=static&x= XSS attack.	2017-03-31	4.3	CVE-2017-7361 MISC (link is external)

				BID (link is external)
getpixie -- pixie	Pixie 1.0.4 allows an admin/index.php s=publish&m=dynamic&x= XSS attack.	2017-03-31	4.3	CVE-2017-7362 MISC (link is external) BID (link is external)
getpixie -- pixie	Pixie 1.0.4 allows an admin/index.php s=publish&m=module&x= XSS attack.	2017-03-31	4.3	CVE-2017-7363 MISC (link is external) BID (link is external)
hak5 -- wi-fi_pineapple_firmware	Hak5 WiFi Pineapple 2.0 through 2.3 uses predictable CSRF tokens.	2017-03-31	4.3	CVE-2015-4624 MISC (link is external) MISC (link is external) BUGTRAQ (link is external) EXPLOIT-DB (link is external)
helpmewatchwho_project -- helpmewatchwho	TheFirstQuestion/HelpMeWatchWho before 2017-03-28 is vulnerable to a reflected XSS in HelpMeWatchWho-master/unaired.php (episodeID parameter).	2017-03-31	4.3	CVE-2017-7387 BID (link is external) CONFIRM (link is external)
huawei -- ascend_p6_edge-t00_firmware	Apps on Huawei Ascend P6 mobile phones with software EDGE-U00 V100R001C17B508SP01 and earlier versions before V100R001C17B508SP02; EDGE-T00 V100R001C01B508SP01 and earlier versions before V100R001C01B508SP02; EDGE-C00 V100R001C92B508SP02 and earlier versions before V100R001C92B508SP03 can capture screens without the root permission. As a result, user information can be leaked by malware on Ascend P6 mobile phones.	2017-04-02	4.3	CVE-2014-8571 CONFIRM (link is external)
huawei -- cloudengine_6800_firmware	Huawei CloudEngine 6800 V100R006C00, CloudEngine 7800 V100R006C00, CloudEngine 8800 V100R006C00, and CloudEngine 12800 V100R006C00 allow remote attackers with specific permission to store massive files to exhaust the shared storage space, leading to a DoS condition.	2017-04-02	6.8	CVE-2016-8780 CONFIRM (link is external) BID (link is external)
huawei -- espace_iad_firmwar	Huawei eSpace IAD V300R002C01SPC100 and earlier versions have an information leak	2017-04-02	5.0	CVE-2016-8271 CONFIRM (link

e	vulnerability; an attacker can check and download the fault information by accessing a special URL.			is external)
huawei -- espace_integrated_access_device_firmware	Huawei eSpace Integrated Access Device (IAD) with software V300R001C03, V300R001C04, V300R001C06, V300R001C20, and V300R001C07 allows an attacker to trick a user into clicking a URL containing malicious scripts to obtain user information or hijack the session, aka XSS.	2017-04-02	4.3	CVE-2016-8789 CONFIRM (link is external) BID (link is external)
huawei -- espace_meeting	In Huawei eSpace Meeting with software V100R001C03SPC201 and the earlier versions, attackers that obtain the permissions assigned to common users can elevate privileges to access and set specific key resources.	2017-04-02	6.6	CVE-2014-3222 CONFIRM (link is external)
huawei -- eudemon8000e_firmware	Huawei Eudemon8000E firewall with software V200R001C01SPC800 and earlier versions allows users to log in to the device using Telnet or SSH. When an attacker sends to the device a mass of TCP packets with special structure, the logging process becomes slow and users may be unable to log in to the device.	2017-04-02	5.0	CVE-2014-3221 CONFIRM (link is external)
huawei -- fusionaccess	Huawei FusionAccess with software V100R005C10 and V100R005C20 could allow remote attackers with specific permission to inject a Lightweight Directory Access Protocol (LDAP) operation command into a specific input variable to obtain sensitive information from the database.	2017-04-02	4.0	CVE-2016-8779 CONFIRM (link is external) BID (link is external)
huawei -- fusionstorage	The maintenance module in Huawei FusionStorage V100R003C30U1 allows attackers to create documents according to special rules to obtain the OS root privilege of FusionStorage.	2017-04-02	4.1	CVE-2016-8803 CONFIRM (link is external) BID (link is external)
huawei -- hisuite	Huawei PC client software HiSuite 4.0.5.300_OVE uses insecure HTTP for upgrade software package download and does not check the integrity of the software package before installing; an attacker can launch an MITM attack to interrupt or replace the downloaded software package and further compromise the PC.	2017-04-02	6.9	CVE-2016-8273 CONFIRM (link is external)
huawei -- logcenter	Huawei LogCenter V100R001C10 could allow an	2017-04-02	4.0	CVE-2015-8670

	authenticated attacker to add abnormal device information to the log collection module, causing denial of service.			CONFIRM (link is external)
huawei -- logcenter	Huawei LogCenter V100R001C10 could allow an authenticated attacker to tamper with requests using a tool and submit a request to the server for privilege escalation, affecting some system functions.	2017-04-02	6.5	CVE-2015-8671 CONFIRM (link is external)
huawei -- mate_s_firmware	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege.	2017-04-02	6.2	CVE-2016-8791 CONFIRM (link is external) BID (link is external)
huawei -- mate_s_firmware	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege.	2017-04-02	6.2	CVE-2016-8792 CONFIRM (link is external) BID (link is external)
huawei --	Huawei Mate 8 phones with software Versions	2017-04-02	6.2	CVE-2016-8793

mate_s_firmware	before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege.			CONFIRM (link is external) BID (link is external)
huawei -- mate_s_firmware	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege.	2017-04-02	6.2	CVE-2016-8794 CONFIRM (link is external) BID (link is external)
huawei -- oceanstor_5600_v3_firmware	Huawei OceanStor 5600 V3 V300R003C00 has a hardcoded SSH key vulnerability; the hardcoded keys are used to encrypt communication data and authenticate different nodes of the devices. An attacker may obtain the hardcoded keys and log in to such a device through SSH.	2017-04-02	5.4	CVE-2016-8754 CONFIRM (link is external) BID (link is external)
huawei -- oceanstor_5800_v3_firmware	The Huawei OceanStor 5800 V300R003C00 has an integer overflow vulnerability. An authenticated attacker may send massive abnormal Network File System (NFS) packets, causing an anomaly in	2017-04-02	4.0	CVE-2016-6177 CONFIRM (link is external)

	specific disk arrays.			
huawei -- p7-l10_firmware	The MeWidget module on Huawei P7 smartphones with software P7-L10 V100R001C00B136 and earlier versions could lead to the disclosure of contact information.	2017-04-02	4.3	CVE-2015-2246 CONFIRM (link is external)
huawei -- p8_lite_firmware	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an input validation vulnerability, which allows attackers to read and write user-mode memory data anywhere in the TrustZone driver.	2017-04-02	4.1	CVE-2016-8764 CONFIRM (link is external) BID (link is external)
huawei -- secospace_usg6300_firmware	Huawei Secospace USG6300 with software V500R001C20 and V500R001C20SPC200PWE, Secospace USG6500 with software V500R001C20, Secospace USG6600 with software V500R001C20 and V500R001C20SPC200PWE allow remote attackers with specific permission to log in to a device and deliver a large number of unspecified commands to exhaust memory, causing a DoS condition.	2017-04-02	4.0	CVE-2016-8781 CONFIRM (link is external) BID (link is external)
huawei -- secospace_usg6300_firmware	The security policy processing module in Huawei Secospace USG6300 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200; Secospace USG6500 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200; Secospace USG6600 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200 allows authenticated attackers to setup a specific security policy into the devices, causing a buffer overflow and crashing the system.	2017-04-02	6.8	CVE-2016-8802 CONFIRM (link is external) BID (link is external)
huawei -- tecal_bh621_v2_firmware	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal	2017-04-02	4.0	CVE-2014-9691 CONFIRM (link is external)

	RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions could allow users who log in to the products to view the sessions IDs of all online users on the Online Users page of the web UI.			

huawei -- tecal_bh621_v2_firmware	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3	2017-04-02	5.0	CVE-2014-9692 CONFIRM (link is external)

	V100R001C00SPC110 and earlier versions could allow attackers to figure out the RMCP+ session IDs of users and access the system with forged identities.			
huawei -- tecal_bh621_v2_firmware	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions,	2017-04-02	6.8	CVE-2014-9694 CONFIRM (link is external)

	Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions have a CSRF vulnerability. The products do not use the Token mechanism for web access control. When users log in to the Huawei servers and access websites containing the malicious CSRF script, the CSRF script is executed, which may cause configuration tampering and system restart.			
huawei -- tecal_e9000_chassis_firmware	The Hyper Module Management (HMM) software of Huawei Tecal E9000 Chassis V100R001C00SPC160 and earlier versions could allow a non-super-domain user who accesses HMM through SNMPv3 to perform operations on a server as a super-domain user.	2017-04-02	6.5	CVE-2014-9695 CONFIRM (link is external)
huawei -- tecal_e9000_chassis_firmware	The Hyper Module Management (HMM) software of Huawei Tecal E9000 Chassis V100R001C00SPC160 and earlier versions allows the operator to modify the user configuration of iMana through privilege escalation.	2017-04-02	6.5	CVE-2014-9696 CONFIRM (link is external)
huawei -- usg2100_firmware	Huawei FusionManager with software V100R002C03 and V100R003C00 could allow an unauthenticated, remote attacker to conduct a CSRF attack against the user of the web interface.	2017-04-02	6.8	CVE-2014-9136 CONFIRM (link is external)
huawei -- usg2100_firmware	Huawei USG9500 with software V200R001C01SPC800 and earlier versions, V300R001C00; USG2100 with software V300R001C00SPC900 and earlier versions; USG2200 with software V300R001C00SPC900; USG5100 with software V300R001C00SPC900 could allow an unauthenticated, remote attacker to conduct a CSRF attack against the user of the web interface.	2017-04-02	6.8	CVE-2014-9137 CONFIRM (link is external)
huawei -- ws318_firmware	Huawei home gateways WS318 with software V100R001C01B022 and earlier versions are affected by the PIN offline brute force cracking vulnerability of the WPS protocol because the random number	2017-04-02	5.0	CVE-2014-9690 CONFIRM (link is external)

	generator (RNG) used in the supplier's solution is not random enough. As a result, brute force cracking the PIN code is easier. After an attacker cracks the PIN, the attacker can access the Internet via the cracked device.			
ibm -- algo_one	IBM Algorithmics One-Algo Risk Application 4.9.1, 5.0, and 5.1.0 could allow a user to gain access to files in the local environment which should not be viewed by application users. IBM Reference #: 1999892.	2017-03-31	4.0	CVE-2017-1154 CONFIRM (link is external) BID (link is external)
ibm -- inotes	IBM iNotes 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1998824.	2017-03-31	4.3	CVE-2016-9990 CONFIRM (link is external) BID (link is external)
ibm -- sterling_selling_and_fulfillment_foundation	IBM Sterling Order Management 9.2 - 9.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 2000943.	2017-03-31	6.8	CVE-2016-8917 CONFIRM (link is external) BID (link is external)
ibm -- tririga_application_platform	The IBM TRIRIGA Application Platform 3.3, 3,4, and 3,5 contain a vulnerability that could allow an authenticated user to execute Application actions they do not have access to. IBM Reference #: 2001083.	2017-03-31	4.0	CVE-2017-1171 BID (link is external) CONFIRM (link is external)
libarchive -- libarchive	The archive_wstring_append_from_mbs function in archive_string.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted archive file.	2017-04-03	4.3	CVE-2016-10209 BID (link is external) CONFIRM (link is external)
magmi_project -- magmi	A Cross-Site Scripting (XSS) was discovered in 'Magmi 0.7.22'. The vulnerability exists due to insufficient filtration of user-supplied data (prefix) passed to the 'magmi-git-master/magmi/web/ajax_gettime.php' URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable	2017-03-31	4.3	CVE-2017-7391 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	website.			
mcafee -- anti-malware_scan_engine	Software Integrity Attacks vulnerability in Intel Security Anti-Virus Engine (AVE) 5200 through 5800 allows local attackers to bypass local security protection via a crafted input file.	2017-03-31	4.4	CVE-2016-8032 BID (link is external) CONFIRM (link is external)
nagios -- nagios	Cross-site scripting (XSS) vulnerability in Nagios.	2017-03-31	4.3	CVE-2016-6209 FULLDISC CONFIRM (link is external)
ni -- labview	An exploitable memory corruption vulnerability exists in the LvVarientUnflatten functionality of LabVIEW 2016 version 16.0.0.49152. A specially crafted VI file can cause a user controlled value to be used as a loop terminator resulting in internal heap corruption. An attacker controlled VI file can be used to trigger this vulnerability, exploitation could lead to remote code execution.	2017-03-31	6.8	CVE-2017-2775 BID (link is external) MISC (link is external)
openeclass_project -- openeclass	Multiple Cross-Site Scripting (XSS) were discovered in 'openeclass Release_3.5.4'. The vulnerabilities exist due to insufficient filtration of user-supplied data (meeting_id, user) passed to the 'openeclass-master/modules/tc/webconf/webconf.php' URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-31	4.3	CVE-2017-7389 BID (link is external) CONFIRM (link is external)
podofo_project -- podofo	The PoDoFo::PdfPainter::ExpandTabs function in PdfPainter.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PDF document.	2017-04-03	4.3	CVE-2017-7378 BID (link is external) MISC
podofo_project -- podofo	The PoDoFo::PdfSimpleEncoding::ConvertToEncoding function in PdfEncoding.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PDF document.	2017-04-03	4.3	CVE-2017-7379 BID (link is external) MISC
podofo_project -- podofo	The doc/PdfPage.cpp:609:23 code in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash)	2017-04-03	4.3	CVE-2017-7381 BID (link is external) MISC

	via a crafted PDF document.			
socialnetwork_project -- socialnetwork	A Cross-Site Scripting (XSS) was discovered in 'SocialNetwork v1.2.1'. The vulnerability exists due to insufficient filtration of user-supplied data (mail) passed to the 'SocialNetwork-andrea/app/template/pw_forgot.php' URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-31	4.3	CVE-2017-7390 BID (link is external) CONFIRM (link is external)
symetrie_project -- symetrie	citymont/symetrie v.0.9.6 is vulnerable to a reflected XSS in symetrie-master/app/commands/page.php (model parameter).	2017-03-31	4.3	CVE-2017-7386 CONFIRM (link is external)
tigervnc -- tigervnc	In TigerVNC 1.7.1 (SSecurityVeNCrypt.cxx SSecurityVeNCrypt::SSecurityVeNCrypt), an unauthenticated client can cause a small memory leak in the server.	2017-03-31	5.0	CVE-2017-7392 BID (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	In TigerVNC 1.7.1 (VNCSConnectionST.cxx VNCSConnectionST::fence), an authenticated client can cause a double free, leading to denial of service or potentially code execution.	2017-03-31	6.5	CVE-2017-7393 BID (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	In TigerVNC 1.7.1 (SSecurityPlain.cxx SSecurityPlain::processMsg), unauthenticated users can crash the server by sending long usernames.	2017-03-31	5.0	CVE-2017-7394 BID (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	In TigerVNC 1.7.1 (SMsgReader.cxx SMsgReader::readClientCutText), by causing an integer overflow, an authenticated client can crash the server.	2017-03-31	4.0	CVE-2017-7395 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	In TigerVNC 1.7.1 (CConnection.cxx CConnection::CConnection), an unauthenticated client can cause a small memory leak in the server.	2017-03-31	5.0	CVE-2017-7396 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
wallacepos_project -- wallacepos	A Cross-Site Scripting (XSS) was discovered in 'wallacepos v1.4.1'. The vulnerability exists due to	2017-03-31	4.3	CVE-2017-7388 BID (link is

	insufficient filtration of user-supplied data (token) passed to the 'wallacepos-master/myaccount/resetpassword.php' URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.			external) CONFIRM (link is external)

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves mishandling of deletion within the SQLite subsystem of the "Safari" component. It allows local users to identify the web-site visits that occurred in Private Browsing mode.	2017-04-01	2.1	CVE-2017-2384 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves symlink mishandling in the "libarchive" component. It allows local users to change arbitrary directory permissions via unspecified vectors.	2017-04-01	2.1	CVE-2017-2390 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Accounts" component. It allows physically proximate attackers to discover an Apple ID by reading an iCloud authentication prompt on the lock screen.	2017-04-01	2.1	CVE-2017-2397 BID (link is external) CONFIRM (link is external)

apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Pasteboard" component. It allows physically proximate attackers to read the pasteboard by leveraging the use of an encryption key derived only from the hardware UID (rather than that UID in addition to the user passcode).	2017-04-01	2.1	CVE-2017-2399 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Siri" component. It allows physically proximate attackers to read text messages on the lock screen via unspecified vectors.	2017-04-01	2.1	CVE-2017-2452 BID (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. The issue involves cleartext client-certificate transmission in the "APNs Server" component. It allows man-in-the-middle attackers to track users via correlation with this certificate.	2017-04-01	3.5	CVE-2017-2383 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves mishandling of DMA in the "EFI" component. It allows physically proximate attackers to discover the FileVault 2 encryption password via a crafted Thunderbolt adapter.	2017-04-01	2.1	CVE-2016-7585 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Hypervisor" component. It allows guest OS users to obtain sensitive information from the CR8 control register via unspecified vectors.	2017-04-01	2.1	CVE-2017-2418 BID (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "Safari Login AutoFill" component. It allows local users to obtain access to locked keychain items via unspecified vectors.	2017-04-01	2.1	CVE-2017-2385 BID (link is external) CONFIRM (link is external)
huawei -- anyoffice	Huawei AnyOffice V200R006C00 could allow an authenticated, remote attacker to cause the software to deny services by uploading an XML	2017-04-02	3.5	CVE-2016-8275 CONFIRM (link is external) BID (link is

	bomb.			external)
huawei -- hisuite	Huawei PC client software HiSuite 4.0.5.300_OVE has an information leak vulnerability; an attacker who can log in to the system can copy out the user's proxy password, causing information leaks.	2017-04-02	2.1	CVE-2016-8272 CONFIRM (link is external)
huawei -- p8_lite_firmware	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an input validation vulnerability, which allows attackers to cause the system to restart.	2017-04-02	1.9	CVE-2016-8762 CONFIRM (link is external) BID (link is external)
ibm -- kenexa_lms	IBM Kenexa LMS on Cloud 13.1, 13.2, 13.2.2, 13.2.3, 13.2.4 and 14.0.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999483.	2017-03-31	3.5	CVE-2016-8935 CONFIRM (link is external) BID (link is external)
ibm -- rational_quality_manager	IBM Quality Manager (RQM) 4.0, 5.0, and 6.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 2000784.	2017-03-31	3.5	CVE-2016-6022 BID (link is external) CONFIRM (link is external)
ibm -- rational_quality_manager	IBM Rational Quality Manager 4.0, 5.0, and 6.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 2000784.	2017-03-31	3.5	CVE-2016-6031 BID (link is external) CONFIRM (link is external)
ibm -- rational_quality_manager	IBM Rational Quality Manager (RQM) 4.0, 5.0, and 6.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 2000784.	2017-03-31	3.5	CVE-2016-6036 BID (link is external) CONFIRM (link is external)

mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the MantisBT Configuration Report page (adm_config_report.php) allows remote attackers to inject arbitrary code through a crafted 'action' parameter. This is fixed in 1.3.8, 2.1.2, and 2.2.2.	2017-03-31	3.5	CVE-2017-6973 CONFIRM (link is external) CONFIRM BID (link is external)
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the MantisBT Move Attachments page (move_attachments_page.php, part of admin tools) allows remote attackers to inject arbitrary code through a crafted 'type' parameter, if Content Security Protection (CSP) settings allows it. This is fixed in 1.3.9, 2.1.3, and 2.2.3. Note that this vulnerability is not exploitable if the admin tools directory is removed, as recommended in the "Post-installation and upgrade tasks" of the MantisBT Admin Guide. A reminder to do so is also displayed on the login page.	2017-03-31	3.5	CVE-2017-7241 CONFIRM (link is external) CONFIRM BID (link is external)
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the MantisBT Configuration Report page (adm_config_report.php) allows remote attackers to inject arbitrary code (if CSP settings permit it) through a crafted 'config_option' parameter. This is fixed in 1.3.9, 2.1.3, and 2.2.3.	2017-03-31	3.5	CVE-2017-7309 CONFIRM (link is external) CONFIRM BID (link is external)

- Sources: http://nvd.nist.gov (For more information visit the National Vulnerabilities Database (NVD) which contains a database of every vulnerability that has ever been published).