Vulnerability Summary for the Week of February 20, 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**
aerospike -- database_server	An exploitable out-of-bounds write vulnerability exists in the batch transaction field parsing functionality of Aerospike Database Server 3.10.0.3. A specially crafted packet can cause an out-of-bounds write resulting in memory corruption which can lead to remote code execution. An attacker can simply connect to the port to trigger this vulnerability.	2017-02-21	7.5	CVE-2016-9051 MISC (link is external)
aerospike -- database_server	An exploitable out-of-bounds indexing vulnerability exists within the RW fabric message particle type of Aerospike Database Server 3.10.0.3. A specially crafted packet can cause the server to fetch a function table outside the bounds of an array resulting in remote code execution. An attacker can simply connect to the port to trigger this vulnerability.	2017-02-21	7.5	CVE-2016-9053 MISC (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "WebSheet" component, which allows attackers to bypass a sandbox protection	2017-02-20	7.5	CVE-2016-7630 CONFIRM (link is external)

	mechanism via unspecified vectors.			
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.1 is affected. The issue involves the "AppleGraphicsControl" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-02-20	9.3	CVE-2016-4662 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "Kernel" component. It allows local users to execute arbitrary code in a privileged context or cause a denial of service (MIG code mishandling and system crash) via unspecified vectors.	2017-02-20	7.2	CVE-2016-4669 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 10.12.1 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write and application crash) via a crafted PDF file.	2017-02-20	9.3	CVE-2016-4671 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "libxpc" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-02-20	9.3	CVE-2016-4675 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 10.12.1 is affected. The issue involves the "Thunderbolt" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app.	2017-02-20	9.3	CVE-2016-4780 CONFIRM (link is external)

apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12 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.	2017-02-20	9.3	CVE-2016-7582 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 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.	2017-02-20	9.3	CVE-2016-7596 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 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.	2017-02-20	9.3	CVE-2016-7602 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app that leverages object-lifetime mishandling during process spawning.	2017-02-20	9.3	CVE-2016-7613 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 10.12.2 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 (type confusion) via a crafted app.	2017-02-20	9.3	CVE-2016-7617 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "kext tools" component. It	2017-02-20	9.3	CVE-2016-7629 BID (link is external) CONFIRM (link

	allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.			is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "Directory Services" component. It allows local users to gain privileges or cause a denial of service (use-after-free) via unspecified vectors.	2017-02-20	7.2	CVE-2016-7633 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. The issue involves the "Power Management" component. It allows local users to gain privileges via unspecified vectors related to Mach port name references.	2017-02-20	7.2	CVE-2016-7661 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 10.12.3 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.	2017-02-20	9.3	CVE-2017-2353 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.3 is affected. The issue involves the "Graphics Drivers" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-02-20	9.3	CVE-2017-2358 BID (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "IOHIDFamily" 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.	2017-02-20	9.3	CVE-2016-7591 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3	2017-02-20	9.3	CVE-2016-7606 BID (link is external) CONFIRM (link

	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.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 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.	2017-02-20	9.3	CVE-2016-7612 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Disk Images" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-02-20	9.3	CVE-2016-7616 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Kernel" component. It allows local users to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via unspecified vectors.	2017-02-20	7.2	CVE-2016-7621 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Kernel" component. It allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	2017-02-20	7.2	CVE-2016-7637 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS	2017-02-20	9.3	CVE-2016-7644 BID (link is external)

	before 10.12.2 is affected. watchOS before 3.1.3 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.			CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "syslog" component. It allows local users to gain privileges via unspecified vectors related to Mach port name references.	2017-02-20	7.2	CVE-2016-7660 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "CoreFoundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted string.	2017-02-20	7.5	CVE-2016-7663 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. macOS before 10.12.3 is affected. tvOS before 10.1.1 is affected. watchOS before 3.1.3 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.	2017-02-20	9.3	CVE-2017-2360 BID (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. macOS before 10.12.3 is affected. tvOS before 10.1.1 is affected. watchOS before 3.1.3 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 (buffer overflow) via a crafted app.	2017-02-20	9.3	CVE-2017-2370 BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

				CONFIRM (link is external)
cmsmadesimple -- form_builder	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to execute PHP code via the cntnt01fbrp_forma_form_template parameter in admin_store_form.	2017-02-21	7.5	CVE-2017-6070 MISC MISC (link is external)
dell -- sonicwall_secure_remote_access_server	The SonicWall Secure Remote Access server (version 8.1.0.2-14sv) is vulnerable to two Remote Command Injection vulnerabilities in its web administrative interface. These vulnerabilities occur in the diagnostics CGI (/cgi-bin/diagnostics) component responsible for emailing out information about the state of the system. The application doesn't properly escape the information passed in the 'tsrDeleteRestartedFile' or 'currentTSREmailTo' variables before making a call to system(), allowing for remote command injection. Exploitation of this vulnerability yields shell access to the remote machine under the nobody user account.	2017-02-22	10.0	CVE-2016-9682 CONFIRM (link is external)
dell -- sonicwall_secure_remote_access_server	The SonicWall Secure Remote Access server (version 8.1.0.2-14sv) is vulnerable to a Remote Command Injection vulnerability in its web administrative interface. This vulnerability occurs in the 'extensionsettings' CGI (/cgi-bin/extensionsettings) component responsible for handling some of the server's internal configurations. The CGI application doesn't properly escape the information it's passed when processing a particular multi-part form request involving scripts. The filename of the 'scriptname' variable is read in unsanitized before a call to system() is performed - allowing for remote command injection. Exploitation of this vulnerability yields shell access to the remote machine under the nobody user account. This is SonicWall Issue ID 181195.	2017-02-22	10.0	CVE-2016-9683 CONFIRM (link is external) MISC (link is external)

dell -- sonicwall_secure_remote_access_server	The SonicWall Secure Remote Access server (version 8.1.0.2-14sv) is vulnerable to a Remote Command Injection vulnerability in its web administrative interface. This vulnerability occurs in the 'viewcert' CGI (/cgi-bin/viewcert) component responsible for processing SSL certificate information. The CGI application doesn't properly escape the information it's passed in the 'CERT' variable before a call to system() is performed - allowing for remote command injection. Exploitation of this vulnerability yields shell access to the remote machine under the nobody user account.	2017-02-22	10.0	CVE-2016-9684 CONFIRM (link is external) MISC (link is external)
disksavvy -- disksavvy_enterprise	Buffer overflow in the built-in web server in DiskSavvy Enterprise 9.4.18 allows remote attackers to execute arbitrary code via a long URI in a GET request.	2017-02-22	7.5	CVE-2017-6187 EXPLOIT-DB (link is external)
dlink -- websmart_dgs-1510_series_firmware	D-Link DGS-1510-28XMP, DGS-1510-28X, DGS-1510-52X, DGS-1510-52, DGS-1510-28P, DGS-1510-28, and DGS-1510-20 Websmart devices with firmware before 1.31.B003 allow attackers to conduct Unauthenticated Command Bypass attacks via unspecified vectors.	2017-02-23	7.5	CVE-2017-6205 CONFIRM (link is external)
facebook -- hhvm	Out-of-bounds write in the (1) mb_detect_encoding, (2) mb_send_mail, and (3) mb_detect_order functions in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors.	2017-02-17	7.5	CVE-2016-6870 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
facebook -- hhvm	Integer overflow in bcmath in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors, which triggers a buffer overflow.	2017-02-17	7.5	CVE-2016-6871 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
facebook -- hhvm	Integer overflow in StringUtil::implode in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors.	2017-02-17	7.5	CVE-2016-6872 MLIST (link is external) MLIST (link is external) CONFIRM (link

				is external)
facebook -- hhvm	Self recursion in compact in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors.	2017-02-17	7.5	CVE-2016-6873 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
facebook -- hhvm	The array_*_recursive functions in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors, related to recursion.	2017-02-17	7.5	CVE-2016-6874 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
facebook -- hhvm	Infinite recursion in wddx in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors.	2017-02-17	7.5	CVE-2016-6875 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
linux -- linux_kernel	Integer overflow in the mem_check_range function in drivers/infiniband/sw/rxe/rxe_mr.c in the Linux kernel before 4.9.10 allows local users to cause a denial of service (memory corruption), obtain sensitive information from kernel memory, or possibly have unspecified other impact via a write or read request involving the "RDMA protocol over infiniband" (aka Soft RoCE) technology.	2017-02-22	7.2	CVE-2016-8636 CONFIRM CONFIRM MLIST (link is external) CONFIRM (link is external) MISC (link is external) CONFIRM (link is external)
linux -- linux_kernel	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.	2017-02-18	7.1	CVE-2017-5986 CONFIRM CONFIRM MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware	2017-02-18	7.6	CVE-2017-6001 CONFIRM CONFIRM MLIST (link is external) CONFIRM (link is external)

	context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.			CONFIRM (link is external)
linux -- linux_kernel	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.	2017-02-18	9.3	CVE-2017-6074 MLIST (link is external) CONFIRM (link is external)
mail-masta -- mail-masta_plugin	A SQL injection issue was discovered in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects /inc/lists/csvexport.php (Unauthenticated) with the GET Parameter: list_id.	2017-02-21	7.5	CVE-2017-6095 MISC (link is external)
metalgenix -- genixcms	CSRF token bypass in GeniXCMS before 1.0.2 could result in escalation of privileges. The forgotpassword.php page can be used to acquire a token.	2017-02-21	7.5	CVE-2017-5959 CONFIRM (link is external) CONFIRM (link is external)
netgear -- dgn2200_firmware	ping.cgi on NETGEAR DGN2200 devices with firmware through 10.0.0.50 allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the ping_IPAddr field of an HTTP POST request.	2017-02-22	10.0	CVE-2017-6077 EXPLOIT-DB (link is external)
trendmicro -- interscan_web_security_virtual_appliance	Remote Command Execution in com.trend.iwss.gui.servlet.ManagePatches in Trend Micro Interscan Web Security Virtual Appliance (IWSVA) version 6.5-SP2_Build_Linux_1707 and earlier allows authenticated, remote users with least privileges to run arbitrary commands on the system as root via Patch Update functionality. This was resolved in Version 6.5 CP 1737.	2017-02-21	9.0	CVE-2016-9269 CONFIRM (link is external)
zyxel -- usg50_firmware	Zyxel USG50 Security Appliance and NWA3560-N Access Point allow remote attackers to cause a denial of service (CPU consumption) via a flood of ICMPv4 Port Unreachable packets.	2017-02-21	7.8	CVE-2016-10227 MISC (link is external) MISC (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
aerospike -- database_server	An exploitable denial-of-service vulnerability exists in the fabric-worker component of Aerospike Database Server 3.10.0.3. A specially crafted packet can cause the server process to dereference a null pointer. An attacker can simply connect to a TCP port in order to trigger this vulnerability.	2017-02-21	5.0	CVE-2016-9049 MISC (link is external)
apple -- apple_tv	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 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.	2017-02-20	4.3	CVE-2017-2350 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- apple_tv	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 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.	2017-02-20	6.8	CVE-2017-2362 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- apple_tv	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 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.	2017-02-20	4.3	CVE-2017-2365 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- apple_tv	An issue was discovered in certain Apple products.	2017-02-20	6.8	CVE-2017-2369

	iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 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.			BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- apple_tv	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 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.	2017-02-20	6.8	CVE-2017-2373 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- garageband	An issue was discovered in certain Apple products. GarageBand before 10.1.6 is affected. The issue involves the "Projects" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted GarageBand project file.	2017-02-20	6.8	CVE-2017-2374 CONFIRM (link is external)
apple -- icloud	An issue was discovered in certain Apple products. iCloud before 6.0.1 is affected. The issue involves the setup subsystem in the "iCloud" component. It allows local users to gain privileges via a crafted dynamic library in an unspecified directory.	2017-02-20	4.6	CVE-2016-7583 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "Sandbox Profiles" component, which allows attackers to read photo-directory metadata via a crafted app.	2017-02-20	4.3	CVE-2016-4664 BID (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 10.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "Sandbox Profiles" component, which allows attackers to read audio-recording metadata via a crafted app.	2017-02-20	4.3	CVE-2016-4665 BID (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 10.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "Kernel" component. It allows attackers to obtain sensitive information from kernel memory via a crafted app.	2017-02-20	4.3	CVE-2016-4680 BID (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 10.1 is affected. The issue involves the "iTunes Backup" component, which improperly hashes passwords, making it easier to decrypt files.	2017-02-20	4.3	CVE-2016-4685 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Mail" component, which does not alert the user to an S/MIME email signature that used a revoked certificate.	2017-02-20	5.0	CVE-2016-4689 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Image Capture" component, which allows attackers to execute arbitrary code via a crafted USB HID device.	2017-02-20	4.6	CVE-2016-4690 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "SpringBoard" component, which allows physically proximate attackers to bypass the passcode attempt counter and unlock a device via unspecified vectors.	2017-02-20	4.6	CVE-2016-4781 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.1 is affected. The issue involves the "Safari" component, which allows remote web servers to cause a denial of service via a crafted URL.	2017-02-20	4.3	CVE-2016-7581 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Local Authentication" component, which does not honor the configured screen-lock time interval if the Touch ID prompt is visible.	2017-02-20	4.6	CVE-2016-7601 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the	2017-02-20	4.3	CVE-2016-7665 BID (link is

	"Graphics Driver" component, which allows remote attackers to cause a denial of service via a crafted video.			external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "WebKit" component, which allows XSS attacks against Safari.	2017-02-20	4.3	CVE-2016-7762 CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. The issue involves the "Contacts" component. It allows remote attackers to cause a denial of service (application crash) via a crafted contact card.	2017-02-20	4.3	CVE-2017-2368 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. The issue involves the "WebKit" component, which allows remote attackers to launch popups via a crafted web site.	2017-02-20	4.3	CVE-2017-2371 BID (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. Safari before 10.0.1 is affected. iCloud before 6.0.1 is affected. iTunes before 12.5.2 is affected. tvOS before 10.0.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a crafted web site.	2017-02-20	4.3	CVE-2016-4613 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iOS before 10 is affected. Safari before 10 is affected. iTunes before 12.5.1 is affected. tvOS before 10 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.	2017-02-20	6.8	CVE-2016-4764 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iOS before 10.1 is affected. Safari before 10.0.1 is affected. iCloud before 6.0.1 is affected. iTunes before 12.5.2 is affected. tvOS before 10.0.1 is affected. The issue involves the "WebKit"	2017-02-20	6.8	CVE-2016-7578 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	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 -- itunes	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 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.	2017-02-20	6.8	CVE-2017-2354 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access and application crash) via a crafted web site.	2017-02-20	6.8	CVE-2017-2355 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 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.	2017-02-20	6.8	CVE-2017-2356 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- itunes	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. The issue involves the	2017-02-20	6.8	CVE-2017-2366 BID (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)
apple -- logic_pro_x	An issue was discovered in certain Apple products. GarageBand before 10.1.5 is affected. Logic Pro X before 10.3 is affected. The issue involves the "Projects" component, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted GarageBand project file.	2017-02-20	6.8	CVE-2017-2372 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 is affected. The issue involves a sandbox escape related to launchctl process spawning in the "libxpc" component.	2017-02-20	4.6	CVE-2016-4617 CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 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.	2017-02-20	5.8	CVE-2016-4660 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 10.12.1 is affected. The issue involves the "ntfs" component, which misparses disk images and allows attackers to cause a denial of service via a crafted app.	2017-02-20	4.3	CVE-2016-4661 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.1 is affected. The issue involves the "NVIDIA Graphics Drivers" component. It allows attackers to cause a denial of service (memory corruption) via a crafted app.	2017-02-20	4.3	CVE-2016-4663 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.1 is affected. The issue involves the "ATS" component. It allows remote attackers to execute arbitrary code or cause a denial of service	2017-02-20	6.8	CVE-2016-4667 BID (link is external) CONFIRM (link is external)

	(memory corruption and application crash) via a crafted font.			
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 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 JPEG file.	2017-02-20	6.8	CVE-2016-4673 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 10.12.1 is affected. The issue involves the "ATS" component. It allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors.	2017-02-20	4.6	CVE-2016-4674 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.1 is affected. The issue involves the "AppleSMC" component. It allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors.	2017-02-20	4.6	CVE-2016-4678 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "libarchive" component, which allows remote attackers to write to arbitrary files via a crafted archive containing a symlink.	2017-02-20	4.3	CVE-2016-4679 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 10.12.1 is affected. The issue involves the "Core Image" 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.	2017-02-20	6.8	CVE-2016-4681 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12 is affected. macOS before	2017-02-20	5.8	CVE-2016-4682 BID (link is external)

	10.12.1 is affected. The issue involves the "ImageIO" 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 SGI file.			CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.1 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds memory access and application crash) via a crafted SGI file.	2017-02-20	6.8	CVE-2016-4683 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. watchOS before 3.1.3 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted font.	2017-02-20	6.8	CVE-2016-4688 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 -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. The issue involves the "IDS - Connectivity" component, which allows man-in-the-middle attackers to spoof calls via a "switch caller" notification.	2017-02-20	4.3	CVE-2016-4721 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. The issue involves the "FaceTime" component, which allows remote attackers to trigger memory corruption and obtain audio data from a call that appeared to have ended.	2017-02-20	4.3	CVE-2016-7577 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. The issue involves the "CFNetwork Proxies" component, which allows man-in-the-middle attackers to spoof	2017-02-20	4.3	CVE-2016-7579 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	a proxy password authentication requirement and obtain sensitive information.			CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12 is affected. The issue involves the "Mail" component, which allows remote web servers to cause a denial of service via a crafted URL.	2017-02-20	4.3	CVE-2016-7580 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. tvOS before 10.0.1 is affected. watchOS before 3.1 is affected. The issue involves the "AppleMobileFileIntegrity" component, which allows remote attackers to spoof signed code by using a matching team ID.	2017-02-20	6.8	CVE-2016-7584 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 10.12.2 is affected. The issue involves the "CoreStorage" component. It allows local users to cause a denial of service (NULL pointer dereference) via unspecified vectors.	2017-02-20	4.9	CVE-2016-7603 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "CoreCapture" component. It allows local users to cause a denial of service (NULL pointer dereference) via unspecified vectors.	2017-02-20	4.9	CVE-2016-7604 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "Bluetooth" component. It allows attackers to cause a denial of service (NULL pointer dereference) via a crafted app.	2017-02-20	4.3	CVE-2016-7605 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "AppleGraphicsPowerManagement" component. It allows local users to cause a denial of service (NULL pointer dereference) via unspecified vectors.	2017-02-20	4.9	CVE-2016-7609 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves	2017-02-20	6.8	CVE-2016-7618 BID (link is external)

	the "Foundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted .gcx file.			CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "Grapher" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted .gcx file.	2017-02-20	6.8	CVE-2016-7622 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. The issue involves the "CoreMedia External Displays" component. It allows local users to gain privileges or cause a denial of service (type confusion) via unspecified vectors.	2017-02-20	6.8	CVE-2016-7655 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to cause a denial of service via a crafted string.	2017-02-20	5.0	CVE-2016-7667 CONFIRM (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "xar" component, which allows remote attackers to execute arbitrary code via a crafted archive that triggers use of uninitialized memory locations.	2017-02-20	6.8	CVE-2016-7742 CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.3 is affected. The issue involves the "IOAudioFamily" component. It allows attackers to obtain sensitive kernel memory-layout information via a crafted app.	2017-02-20	4.3	CVE-2017-2357 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.3 is affected. The issue involves the "Help Viewer" component, which allows XSS attacks via a crafted web site.	2017-02-20	4.3	CVE-2017-2361 BID (link is external) MISC CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products.	2017-02-20	6.8	CVE-2016-4666 BID (link is

	iOS before 10.1 is affected. Safari before 10.0.1 is affected. tvOS before 10.0.1 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.			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 10.1 is affected. Safari before 10.0.1 is affected. tvOS before 10.0.1 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.	2017-02-20	6.8	CVE-2016-4677 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-4692 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information from process memory or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-02-20	5.8	CVE-2016-4743 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a crafted web site.	2017-02-20	4.3	CVE-2016-7586 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7587 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component, which allows remote attackers to obtain sensitive information via crafted JavaScript prompts on a web site.	2017-02-20	4.3	CVE-2016-7592 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information from process memory via a crafted web site.	2017-02-20	4.3	CVE-2016-7598 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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 that uses HTTP redirects.	2017-02-20	4.3	CVE-2016-7599 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute	2017-02-20	6.8	CVE-2016-7610 BID (link is external) CONFIRM (link is external) CONFIRM (link

	arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7611 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 10.2 is affected. Safari before 10.0.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a blob URL on a web site.	2017-02-20	4.3	CVE-2016-7623 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7632 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7635 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit"	2017-02-20	6.8	CVE-2016-7639 BID (link is external) CONFIRM (link is external)

	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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7640 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7641 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7642 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7645 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7646 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7648 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7649 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7652 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 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute	2017-02-20	6.8	CVE-2016-7654 BID (link is external) CONFIRM (link is external) CONFIRM (link

	arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 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.	2017-02-20	6.8	CVE-2016-7656 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. Safari before 10.0.3 is affected. The issue involves the "Safari" component, which allows remote attackers to spoof the address bar via a crafted web site.	2017-02-20	4.3	CVE-2017-2359 BID (link is external) CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 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.	2017-02-20	4.3	CVE-2017-2364 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- transporter	An issue was discovered in certain Apple products. Transporter before 1.9.2 is affected. The issue involves the "iTMSTransporter" component, which allows attackers to obtain sensitive information via a crafted EPUB.	2017-02-20	4.3	CVE-2016-7666 BID (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 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.	2017-02-20	6.8	CVE-2016-4691 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue	2017-02-20	5.0	CVE-2016-4693 BID (link is external) CONFIRM (link

	involves the "Security" component, which makes it easier for attackers to bypass cryptographic protection mechanisms by leveraging use of the 3DES cipher.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "CoreMedia Playback" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted MP4 file.	2017-02-20	6.8	CVE-2016-7588 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. watchOS before 3.1.3 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.	2017-02-20	6.8	CVE-2016-7589 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 -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "ICU" 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.	2017-02-20	6.8	CVE-2016-7594 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 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.	2017-02-20	6.8	CVE-2016-7595 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue	2017-02-20	4.3	CVE-2016-7607 BID (link is external) CONFIRM (link

	involves the "Kernel" component, which allows attackers to obtain sensitive information from kernel memory via a crafted app.			is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Kernel" component, which allows local users to cause a denial of service via unspecified vectors.	2017-02-20	4.9	CVE-2016-7615 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. tvOS before 10.1 is affected. watchOS before 3.1.1 is affected. The issue involves the "Profiles" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted certificate profile.	2017-02-20	6.8	CVE-2016-7626 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "CoreGraphics" component. It allows attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted font.	2017-02-20	4.3	CVE-2016-7627 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Security" component, which allows man-in-the-middle attackers to cause a denial of service (application crash) via vectors related to OCSP responder URLs.	2017-02-20	4.3	CVE-2016-7636 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "ImageIO" component. It allows remote attackers to obtain sensitive information	2017-02-20	5.8	CVE-2016-7643 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	from process memory or cause a denial of service (out-of-bounds read and application crash) via a crafted web site.			CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. watchOS before 3.1.1 is affected. The issue involves the "Accounts" component, which allows local users to bypass intended authorization restrictions by leveraging the mishandling of an app uninstall.	2017-02-20	4.6	CVE-2016-7651 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "IOKit" component. It allows attackers to obtain sensitive information from kernel memory via a crafted app.	2017-02-20	4.3	CVE-2016-7657 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 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 file.	2017-02-20	6.8	CVE-2016-7658 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 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 file.	2017-02-20	6.8	CVE-2016-7659 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "Security" component, which allows remote attackers to spoof certificates via unspecified vectors.	2017-02-20	5.0	CVE-2016-7662 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. watchOS before 3.1.3 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.	2017-02-20	4.3	CVE-2017-2363 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- identity_services_engine_software	A vulnerability in the sponsor portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access notices owned by other users, because of SQL Injection. More Information: CSCvb15627. Known Affected Releases: 1.4(0.908).	2017-02-21	6.5	CVE-2017-3835 CONFIRM (link is external)
cisco -- intrusion_prevention_system_device_manager	A vulnerability in the web-based management interface of the Cisco Intrusion Prevention System Device Manager (IDM) could allow an unauthenticated, remote attacker to view sensitive information stored in certain HTML comments. More Information: CSCuh91455. Known Affected Releases: 7.2(1)V7.	2017-02-21	5.0	CVE-2017-3842 CONFIRM (link is external)
cisco -- meeting_server	A vulnerability in an internal API of the Cisco Meeting Server (CMS) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected appliance. More Information: CSCvc89678. Known Affected Releases: 2.1. Known Fixed Releases: 2.1.2.	2017-02-21	5.0	CVE-2017-3830 CONFIRM (link is external)
cisco -- meeting_server	An HTTP Packet Processing vulnerability in the Web Bridge interface of the Cisco Meeting Server (CMS), formerly Acano Conferencing Server, could allow an authenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information. In addition, the attacker could potentially cause the application to crash unexpectedly, resulting in a denial of service (DoS) condition. The attacker would need to be authenticated and have a valid session with the Web Bridge. Affected Products: This vulnerability	2017-02-21	5.5	CVE-2017-3837 CONFIRM (link is external)

	affects Cisco Meeting Server software releases prior to 2.1.2. This product was previously known as Acano Conferencing Server. More Information: CSCvc89551. Known Affected Releases: 2.0 2.0.7 2.1. Known Fixed Releases: 2.1.2.			
cisco -- prime_collaboration_assurance	A vulnerability in the file download functions for Cisco Prime Collaboration Assurance could allow an authenticated, remote attacker to download system files that should be restricted. More Information: CSCvc99446. Known Affected Releases: 11.5(0).	2017-02-21	4.0	CVE-2017-3843 CONFIRM (link is external)
cisco -- prime_collaboration_assurance	A vulnerability in exporting functions of the user interface for Cisco Prime Collaboration Assurance could allow an authenticated, remote attacker to view file directory listings and download files. Affected Products: Cisco Prime Collaboration Assurance software versions 11.0, 11.1, and 11.5 are vulnerable. Cisco Prime Collaboration Assurance software versions prior to 11.0 are not vulnerable. More Information: CSCvc86238. Known Affected Releases: 11.5(0).	2017-02-21	4.0	CVE-2017-3844 CONFIRM (link is external)
cisco -- prime_collaboration_assurance	A vulnerability in the web-based management interface of Cisco Prime Collaboration Assurance could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. Affected Products: Cisco Prime Collaboration Assurance software versions 11.0, 11.1, and 11.5 are vulnerable. Cisco Prime Collaboration Assurance software versions prior to 11.0 are not vulnerable. More Information: CSCvc77783. Known Affected Releases: 11.5(0).	2017-02-21	4.3	CVE-2017-3845 CONFIRM (link is external)
cisco -- secure_access_control_system	A vulnerability in Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to conduct a DOM-based cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCvc04838. Known Affected Releases: 5.8(2.5).	2017-02-21	4.3	CVE-2017-3838 CONFIRM (link is external)
cisco --	An XML External Entity vulnerability in the web-	2017-02-21	4.0	CVE-2017-3839 CONFIRM (link

secure_access_control_system	based user interface of the Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to have read access to part of the information stored in the affected system. More Information: CSCvc04845. Known Affected Releases: 5.8(2.5).			is external)
cisco -- secure_access_control_system	A vulnerability in the web interface of the Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to redirect a user to a malicious web page, aka an Open Redirect Vulnerability. More Information: CSCvc04849. Known Affected Releases: 5.8(2.5).	2017-02-21	5.8	CVE-2017-3840 CONFIRM (link is external)
cisco -- secure_access_control_system	A vulnerability in the web interface of the Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to disclose sensitive information. More Information: CSCvc04854. Known Affected Releases: 5.8(2.5).	2017-02-21	5.0	CVE-2017-3841 CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the serviceability page of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to conduct reflected cross-site scripting (XSS) attacks. More Information: CSCvc49348. Known Affected Releases: 10.5(2.14076.1). Known Fixed Releases: 12.0(0.98000.209) 12.0(0.98000.478) 12.0(0.98000.609).	2017-02-21	4.3	CVE-2017-3821 CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. More Information: CSCvb98777. Known Affected Releases: 11.0(1.10000.10) 11.5(1.10000.6). Known Fixed Releases: 11.0(1.23063.1) 11.5(1.12029.1) 11.5(1.12900.11) 11.5(1.12900.21) 11.6(1.10000.4) 12.0(0.98000.156) 12.0(0.98000.178) 12.0(0.98000.369) 12.0(0.98000.470) 12.0(0.98000.536) 12.0(0.98000.6) 12.0(0.98500.6).	2017-02-21	4.3	CVE-2017-3828 CONFIRM (link is external)

cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. More Information: CSCvc30999. Known Affected Releases: 12.0(0.98000.280). Known Fixed Releases: 11.0(1.23900.3) 12.0(0.98000.180) 12.0(0.98000.422) 12.0(0.98000.541) 12.0(0.98000.6).	2017-02-21	4.3	CVE-2017-3829 CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of the affected software. More Information: CSCvb95951. Known Affected Releases: 12.0(0.99999.2). Known Fixed Releases: 11.0(1.23064.1) 11.5(1.12031.1) 11.5(1.12900.21) 11.5(1.12900.7) 11.5(1.12900.8) 11.6(1.10000.4) 12.0(0.98000.155) 12.0(0.98000.178) 12.0(0.98000.366) 12.0(0.98000.367) 12.0(0.98000.468) 12.0(0.98000.469) 12.0(0.98000.536) 12.0(0.98000.6) 12.0(0.98500.6).	2017-02-21	4.3	CVE-2017-3833 CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the web framework Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to view sensitive data. More Information: CSCvb61689. Known Affected Releases: 11.5(1.11007.2). Known Fixed Releases: 12.0(0.98000.162) 12.0(0.98000.178) 12.0(0.98000.383) 12.0(0.98000.488) 12.0(0.98000.536) 12.0(0.98000.6) 12.0(0.98500.6).	2017-02-21	4.0	CVE-2017-3836 CONFIRM (link is external)
cmsmadesimple -- form_builder	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via exportxml.	2017-02-21	5.0	CVE-2017-6071 MISC MISC (link is external)
cmsmadesimple -- form_builder	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via defaultadmin.	2017-02-21	5.0	CVE-2017-6072 MISC MISC (link is external)

digisol -- dg-hr1400_firmware	Multiple cross-site request forgery (CSRF) vulnerabilities in the access portal on the DIGISOL DG-HR1400 Wireless Router with firmware 1.00.02 allow remote attackers to hijack the authentication of administrators for requests that (1) change the SSID, (2) change the Wi-Fi password, or (3) possibly have unspecified other impact via crafted requests to form2WlanBasicSetup.cgi.	2017-02-21	6.8	CVE-2017-6127 FULLDISC MISC (link is external)
dlink -- websmart_dgs-1510_series_firmware	D-Link DGS-1510-28XMP, DGS-1510-28X, DGS-1510-52X, DGS-1510-52, DGS-1510-28P, DGS-1510-28, and DGS-1510-20 Websmart devices with firmware before 1.31.B003 allow attackers to conduct Unauthenticated Information Disclosure attacks via unspecified vectors.	2017-02-23	5.0	CVE-2017-6206 CONFIRM (link is external)
faststone -- maxview	FastStone MaxView 3.0 and 3.1 allows user-assisted attackers to cause a denial of service (application crash) via a malformed BMP image with a crafted biSize field in the BITMAPINFOHEADER section.	2017-02-21	4.3	CVE-2017-6078 MISC (link is external)
fedoraproject -- fedora	The route manager in FlightGear before 2016.4.4 allows remote attackers to write to arbitrary files via a crafted Nasal script.	2017-02-22	5.0	CVE-2016-9956 DEBIAN MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) FEDORA FEDORA CONFIRM (link is external) CONFIRM (link is external)
gomlab -- gom_player	GOM Player 2.3.10.5266 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted fpx file.	2017-02-21	6.8	CVE-2017-5881 EXPLOIT-DB (link is external)
google -- chrome	Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video memory, which allowed a remote attacker to possibly extract image fragments on systems with	2017-02-17	4.3	CVE-2017-5017 BID (link is external) CONFIRM (link is external)

	GeForce 8600M graphics chips via a crafted HTML page.			CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5018 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5021 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2017-02-17	4.3	CVE-2017-5024 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
html5lib -- html5lib	The serializer in html5lib before 0.99999999 might allow remote attackers to conduct cross-site scripting (XSS) attacks by leveraging mishandling of the < (less than) character in attribute values.	2017-02-22	4.3	CVE-2016-9909 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
html5lib -- html5lib	The serializer in html5lib before 0.99999999 might allow remote attackers to conduct cross-site scripting (XSS) attacks by leveraging mishandling of special characters in attribute values, a different vulnerability than CVE-2016-9909.	2017-02-22	4.3	CVE-2016-9910 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link

				is external) CONFIRM (link is external) CONFIRM (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 #: 1997010.	2017-02-23	4.3	CVE-2016-5883 CONFIRM (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 could allow an authenticated user to crash the MQ channel due to improper data conversion handling. IBM Reference #: 1998661.	2017-02-22	4.0	CVE-2016-3013 CONFIRM (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0, under nonstandard configurations, sends password data in cleartext over the network that could be intercepted using main in the middle techniques. IBM Reference #: 1998660.	2017-02-22	4.3	CVE-2016-3052 CONFIRM (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 could allow an authenticated user with access to the queue manager and queue, to deny service to other channels running under the same process. IBM Reference #: 1998649.	2017-02-22	4.0	CVE-2016-8915 CONFIRM (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 could allow an authenticated user with access to the queue manager to bring down MQ channels using specially crafted HTTP requests. IBM Reference #: 1998648.	2017-02-22	4.0	CVE-2016-8986 CONFIRM (link is external)
inverse-inc -- sogo	Multiple cross-site scripting (XSS) vulnerabilities in the Web Calendar in SOGo before 2.2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) title of an appointment or (2) contact fields.	2017-02-17	4.3	CVE-2014-9905 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link

				is external)
inverse-inc -- sogo	Incomplete blacklist in SOGo before 2.3.12 and 3.x before 3.1.1 allows remote authenticated users to obtain sensitive information by reading the fields in the (1) ics or (2) XML calendar feeds.	2017-02-17	4.0	CVE-2016-6189 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
inverse-inc -- sogo	SOGo before 2.3.12 and 3.x before 3.1.1 does not restrict access to the UID and DTSTAMP attributes, which allows remote authenticated users to obtain sensitive information about appointments with the "View the Date & Time" restriction, as demonstrated by correlating UIDs and DTSTAMPs between all users.	2017-02-17	4.0	CVE-2016-6190 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
inverse-inc -- sogo	Multiple cross-site scripting (XSS) vulnerabilities in the View Raw Source page in the Web Calendar in SOGo before 3.1.3 allow remote attackers to inject arbitrary web script or HTML via the (1) Description, (2) Location, (3) URL, or (4) Title field.	2017-02-17	4.3	CVE-2016-6191 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The print_frame_inst_bytes function in libdwarf before 20160923 allows remote attackers to cause a denial of service (NULL pointer dereference) via an object file with empty bss-like sections.	2017-02-17	4.3	CVE-2016-5028 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The create_fullest_file_path function in libdwarf before 20160923 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted dwarf file.	2017-02-17	4.3	CVE-2016-5029 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The _dwarf_calculate_info_section_end_ptr function in libdwarf before 20160923 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-02-17	4.3	CVE-2016-5030 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project --	The print_frame_inst_bytes function in libdwarf	2017-02-17	4.3	CVE-2016-5031 MLIST (link is

libdwarf	before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.			external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The dwarf_get_xu_hash_entry function in libdwarf before 20160923 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-02-17	4.3	CVE-2016-5032 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The print_exprloc_content function in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2017-02-17	4.3	CVE-2016-5033 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	dwarf_elf_access.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted file, related to relocation records.	2017-02-17	4.3	CVE-2016-5034 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The _dwarf_read_line_table_header function in dwarf_line_table_reader.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2017-02-17	4.3	CVE-2016-5035 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The dump_block function in print_sections.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via crafted frame data.	2017-02-17	5.0	CVE-2016-5036 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The _dwarf_load_section function in libdwarf before 20160923 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-02-17	4.3	CVE-2016-5037 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project --	The dwarf_get_macro_startend_file function in	2017-02-17	5.0	CVE-2016-5038 MLIST (link is

libdwarf	dwarf_macro5.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted string offset for .debug_str.			external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The get_attr_value function in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted object with all-bits on.	2017-02-17	5.0	CVE-2016-5039 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a large length value in a compilation unit header.	2017-02-17	4.3	CVE-2016-5040 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The dwarf_get_aranges_list function in libdwarf before 20160923 allows remote attackers to cause a denial of service (infinite loop and crash) via a crafted DWARF section.	2017-02-17	5.0	CVE-2016-5042 MLIST (link is external) MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The dwarf_dealloc function in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted DWARF section.	2017-02-17	5.0	CVE-2016-5043 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The WRITE_UNALIGNED function in dwarf_elf_access.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via a crafted DWARF section.	2017-02-17	5.0	CVE-2016-5044 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libdwarf_project -- libdwarf	The read_line_table_program function in dwarf_line_table_reader_common.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via crafted input.	2017-02-17	4.3	CVE-2016-7510 MISC (link is external) CONFIRM (link is external)

libdwarf_project -- libdwarf	Integer overflow in the dwarf_die_deliv.c in libdwarf 20160613 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-02-17	4.3	CVE-2016-7511 CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain rounding operation, which allows local users to map page zero, and consequently bypass a protection mechanism that exists for the mmap system call, by making crafted shmget and shmat system calls in a privileged context.	2017-02-24	4.6	CVE-2017-5669 MISC CONFIRM (link is external)
linux -- linux_kernel	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.	2017-02-23	5.0	CVE-2017-6214 CONFIRM CONFIRM CONFIRM (link is external)
mail-masta -- mail-masta_plugin	A SQL injection issue was discovered in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects /inc/lists/view-list.php (Requires authentication to Wordpress admin) with the GET Parameter: filter_list.	2017-02-21	6.5	CVE-2017-6096 MISC (link is external)
mail-masta -- mail-masta_plugin	A SQL injection issue was discovered in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects /inc/campaign/count_of_send.php (Requires authentication to Wordpress admin) with the POST Parameter: camp_id.	2017-02-21	6.5	CVE-2017-6097 MISC (link is external)
mail-masta -- mail-masta_plugin	A SQL injection issue was discovered in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects /inc/campaign_save.php (Requires authentication to Wordpress admin) with the POST Parameter: list_id.	2017-02-21	6.5	CVE-2017-6098 MISC (link is external)
mantisbt -- mantisbt	Cross-site scripting (XSS) vulnerability in manage_custom_field_edit_page.php in MantisBT 1.2.19 and earlier allows remote attackers to inject arbitrary web script or HTML via the return parameter.	2017-02-17	4.3	CVE-2016-5364 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM

metalgenix -- genixcms	SQL injection vulnerability in inc/lib/Control/Backend/menus.control.php in GeniXCMS through 1.0.2 allows remote authenticated users to execute arbitrary SQL commands via the order parameter.	2017-02-17	6.5	CVE-2017-6065 MISC (link is external)
shadow_project -- shadow	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.	2017-02-17	4.6	CVE-2016-6252 MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
tcpdf_project -- tcpdf	tcpdf before 6.2.0 uploads files from the server generating PDF-files to an external FTP.	2017-02-23	5.0	CVE-2017-6100 MLIST (link is external) CONFIRM CONFIRM (link is external)
tnef_project -- tnef	An issue was discovered in tnef before 1.4.13. Two OOB Writes have been identified in src/mapi_attr.c:mapi_attr_read(). These might lead to invalid read and write operations, controlled by an attacker.	2017-02-23	6.8	CVE-2017-6307 MISC (link is external) MISC (link is external) MISC (link is external)
tnef_project -- tnef	An issue was discovered in tnef before 1.4.13. Several Integer Overflows, which can lead to Heap Overflows, have been identified in the functions that wrap memory allocation.	2017-02-23	6.8	CVE-2017-6308 MISC (link is external) MISC (link is external) MISC (link is external)
tnef_project -- tnef	An issue was discovered in tnef before 1.4.13. Two type confusions have been identified in the parse_file() function. These might lead to invalid read and write operations, controlled by an attacker.	2017-02-23	6.8	CVE-2017-6309 MISC (link is external) MISC (link is external) MISC (link is external)
tnef_project -- tnef	An issue was discovered in tnef before 1.4.13. Four	2017-02-23	6.8	CVE-2017-6310

	type confusions have been identified in the file_add_mapi_attrs() function. These might lead to invalid read and write operations, controlled by an attacker.			MISC (link is external) MISC (link is external) MISC (link is external)
trendmicro -- interscan_web_security_virtual_appliance	Sensitive Information Disclosure in com.trend.iwss.gui.servlet.ConfigBackup in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) version 6.5-SP2_Build_Linux_1707 and earlier allows authenticated, remote users with least privileges to backup the system configuration and download it onto their local machine. This backup file contains sensitive information like passwd/shadow files, RSA certificates, Private Keys and Default Passphrase, etc. This was resolved in Version 6.5 CP 1737.	2017-02-21	4.0	CVE-2016-9314 CONFIRM (link is external)
trendmicro -- interscan_web_security_virtual_appliance	Privilege Escalation Vulnerability in com.trend.iwss.gui.servlet.updateaccountadministration in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) version 6.5-SP2_Build_Linux_1707 and earlier allows authenticated, remote users with least privileges to change Master Admin's password and/or add new admin accounts. This was resolved in Version 6.5 CP 1737.	2017-02-21	4.0	CVE-2016-9315 CONFIRM (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "1 of 9. Null Pointer Deref / calloc return value not checked."	2017-02-23	6.8	CVE-2017-6298 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "2 of 9. Infinite Loop / DoS in the TNEFFillMapi function in lib/ytnef.c."	2017-02-23	4.3	CVE-2017-6299 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "3 of 9. Buffer Overflow in version field in lib/tnef-types.h."	2017-02-23	6.8	CVE-2017-6300 MISC (link is external) MISC (link is

				external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "4 of 9. Out of Bounds Reads."	2017-02-23	6.8	CVE-2017-6301 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "5 of 9. Integer Overflow."	2017-02-23	6.8	CVE-2017-6302 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "6 of 9. Invalid Write and Integer Overflow."	2017-02-23	6.8	CVE-2017-6303 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "7 of 9. Out of Bounds read."	2017-02-23	6.8	CVE-2017-6304 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "8 of 9. Out of Bounds read and write."	2017-02-23	6.8	CVE-2017-6305 MISC (link is external) MISC (link is external) MISC (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "9 of 9. Directory Traversal using the filename; SanitizeFilename function in settings.c."	2017-02-23	6.8	CVE-2017-6306 MISC (link is external) MISC (link is external) MISC (link is external)

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
apple -- icloud	An issue was discovered in certain Apple products. iCloud before 6.1 is affected. The issue involves the "Windows Security" component. It allows local users to obtain sensitive information from iCloud desktop-client process memory via unspecified vectors.	2017-02-20	2.1	CVE-2016-7614 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.1 is affected. The issue involves the "Contacts" component, which does not prevent an app's Address Book access after access revocation.	2017-02-20	3.6	CVE-2016-4686 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "SpringBoard" component, which allows physically proximate attackers to maintain the unlocked state via vectors related to Handoff with Siri.	2017-02-20	2.1	CVE-2016-7597 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Accessibility" component, which accepts spoken passwords without considering that they are locally audible.	2017-02-20	2.1	CVE-2016-7634 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Find My iPhone" component, which allows physically proximate attackers to disable this component by bypassing authentication.	2017-02-20	2.1	CVE-2016-7638 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Media Player" component, which allows physically proximate attackers to obtain sensitive photo and contact information by leveraging lockscreen access.	2017-02-20	2.1	CVE-2016-7653 BID (link is external) CONFIRM (link is external)

apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Accessibility" component. which allows physically proximate attackers to obtain sensitive photo and contact information by leveraging the availability of excessive options during lockscreen access.	2017-02-20	2.1	CVE-2016-7664 BID (link is external) CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10 is affected. The issue involves the "Springboard" component, which allows physically proximate attackers to obtain sensitive information by viewing application snapshots in the Task Switcher.	2017-02-20	2.1	CVE-2016-7759 CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Clipboard" component, which allows physically proximate attackers to obtain sensitive information in the lockscreen state by viewing clipboard contents.	2017-02-20	2.1	CVE-2016-7765 CONFIRM (link is external)
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. The issue involves the "WiFi" component, which allows physically proximate attackers to bypass the activation-lock protection mechanism and view the home screen via unspecified vectors.	2017-02-20	2.1	CVE-2017-2351 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS before 10.12.1 is affected. The issue involves the "Security" component. It allows local users to discover lengths of arbitrary passwords by reading a log.	2017-02-20	2.1	CVE-2016-4670 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 10.12.2 is affected. The issue involves the "OpenPAM" component, which allows local users to obtain sensitive information by leveraging mishandling of failed PAM authentication by a sandboxed app.	2017-02-20	2.1	CVE-2016-7600 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "IOFireWireFamily" component, which allows	2017-02-20	2.1	CVE-2016-7608 BID (link is external) CONFIRM (link

	local users to obtain sensitive information from kernel memory via unspecified vectors.			is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "IOSurface" component. It allows local users to obtain sensitive kernel memory-layout information via unspecified vectors.	2017-02-20	2.1	CVE-2016-7620 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "IOAcceleratorFamily" component. It allows local users to obtain sensitive kernel memory-layout information via unspecified vectors.	2017-02-20	2.1	CVE-2016-7624 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "IOKit" component. It allows local users to obtain sensitive kernel memory-layout information via unspecified vectors.	2017-02-20	2.1	CVE-2016-7625 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "Assets" component, which allows local users to bypass intended permission restrictions and change a downloaded mobile asset via unspecified vectors.	2017-02-20	2.1	CVE-2016-7628 BID (link is external) CONFIRM (link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "WiFi" component, which allows local users to obtain sensitive network-configuration information by leveraging global storage.	2017-02-20	2.1	CVE-2016-7761 CONFIRM (link is external)
apple -- safari	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. The issue involves the "Safari Reader" component, which allows remote attackers to conduct UXSS attacks via a crafted web site.	2017-02-20	2.6	CVE-2016-7650 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "libarchive" component, which allows local users to write to arbitrary files via vectors	2017-02-20	2.1	CVE-2016-7619 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	related to symlinks.			CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS before 10.12.2 is affected. watchOS before 3.1.3 is affected. The issue involves the "IOKit" component. It allows local users to obtain sensitive kernel memory-layout information via unspecified vectors.	2017-02-20	2.1	CVE-2016-7714 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
apple -- watch_os	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. watchOS before 3.1.3 is affected. The issue involves the "Unlock with iPhone" component, which allows attackers to bypass the wrist-presence protection mechanism and unlock a Watch device via unspecified vectors.	2017-02-20	2.1	CVE-2017-2352 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in the web framework of Cisco Firepower Management Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface. More Information: CSCvc72741. Known Affected Releases: 6.2.1.	2017-02-21	3.5	CVE-2017-3847 CONFIRM (link is external)
f5 -- big-ip_application_acceleration_manager	F5 BIG-IP 12.0.0 and 11.5.0 - 11.6.1 REST requests which timeout during user account authentication may log sensitive attributes such as passwords in plaintext to /var/log/restjavad.0.log. It may allow local users to obtain sensitive information by reading these files.	2017-02-20	2.1	CVE-2016-6249 CONFIRM (link is external)
ibm -- rational_requirements_composer	IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 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 #: 1995515.	2017-02-23	3.5	CVE-2016-6055 CONFIRM (link is external)
intersect_alliance -- snare_epilog	Cross-site scripting (XSS) vulnerability in InterSect Alliance SNARE Epilog for UNIX version 1.5 allows remote authenticated users to inject arbitrary web script or HTML via the str_log_name parameter in a "Web Admin Portal > Log Configuration > Add"	2017-02-17	3.5	CVE-2017-5998 MISC (link is external)

	action.			
mantisbt -- mantisbt	MantisBT before 1.3.1 and 2.x before 2.0.0-beta.2 uses a weak Content Security Policy when using the Gravatar plugin, which allows remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.	2017-02-17	2.6	CVE-2016-7111 MLIST (link is external) MLIST (link is external) CONFIRM (link is external) CONFIRM
munin-monitoring -- munin	Munin before 2.999.6 has a local file write vulnerability when CGI graphs are enabled. Setting multiple upper_limit GET parameters allows overwriting any file accessible to the www-data user.	2017-02-22	1.9	CVE-2017-6188 CONFIRM CONFIRM (link is external)
trendmicro -- interscan_web_security_virtual_appliance	Multiple stored Cross-Site-Scripting (XSS) vulnerabilities in com.trend.iwss.gui.servlet.updateaccountadministration in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) version 6.5-SP2_Build_Linux_1707 and earlier allow authenticated, remote users with least privileges to inject arbitrary HTML/JavaScript code into web pages. This was resolved in Version 6.5 CP 1737.	2017-02-21	3.5	CVE-2016-9316 CONFIRM (link is external)
vce_vision -- intelligent_operations	The System Library in VCE Vision Intelligent Operations before 2.6.5 does not properly implement cryptography, which makes it easier for local users to discover credentials by leveraging administrative access.	2017-02-21	2.1	CVE-2015-4056 BUGTRAQ
wolfssl -- wolfssl	In versions of wolfSSL before 3.10.2 the function fp_mul_comba makes it easier to extract RSA key information for a malicious user who has access to view cache on a machine.	2017-02-23	2.1	CVE-2017-6076 CONFIRM (link is external)
xen -- xen	Xen 4.5.x through 4.7.x on AMD systems without the NRip feature, when emulating instructions that generate software interrupts, allows local HVM guest OS users to cause a denial of service (guest crash) by leveraging IDT entry miscalculation.	2017-02-22	2.1	CVE-2016-9377 BID (link is external) CONFIRM
xen -- xen	Xen 4.5.x through 4.7.x on AMD systems without the NRip feature, when emulating instructions that generate software interrupts, allows local HVM guest OS users to cause a denial of service (guest crash) by	2017-02-22	2.1	CVE-2016-9378 BID (link is external) CONFIRM

	leveraging an incorrect choice for software interrupt delivery.			
xen -- xen	Xen 4.7 allows local guest OS users to obtain sensitive host information by loading a 32-bit ELF symbol table.	2017-02-22	2.1	CVE-2016-9384 BID (link is external) CONFIRM CONFIRM

- 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).