National Critical Information Infrastructure Protection Centre

CVE Report

16-28 February 2017 Vol. 04 No. 04

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Aerospike					
Database Server Aerospike Database Server is a flash-optimized, in-memory, nosql database.					
NA	21-02-2017	5	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. **CVE ID: CVE-2016-9049**	NA	A-AER-DATAB-030317/01
Execute Code	21-02-2017	7.5	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. **CVE ID: CVE-2016-9053**	NA	A-AER-DATAB-030317/02
Execute Code; Memory Corruption	21-02-2017	7.5	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. **CVE ID: CVE-2016-9051**	NA	A-AER-DATAB-030317/03

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Apple					
Garageband GarageBand is a whole music creation studio inside your Mac, with a complete sound library that includes software instruments, presets for guitar and voice, and virtual session drummers.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2374**	https://support.apple.com/HT207518	A-APP-GARAG-030317/04
Garageband; Logic Pro X GarageBand is a whole music creation studio inside your Mac ,with a complete sound library that includes software instruments, presets for guitar and voice, and virtual session drummers; Logic Pro X is Apple's professional audio production software and the counterpart to its entry-level Garageband app that comes with Macs and iOS devices.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2372**	https://support.apple.com/HT207477	A-APP-GARAG-030317/05
Icloud iCloud is a cloud storage and cloud computing service from Apple Inc. launched on October 12, 2011.					
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7614**	https://support.apple.com/HT207424	A-APP-ICLOU-030317/06
Gain Privileges	20-02-2017	4.6	An issue was discovered in certain Apple products. iCloud before	https://support.apple.c	A-APP-ICLOU-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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. **CVE ID: CVE-2016-7583**	om/HT207273	030317/07
Safari Safari is Apple's stylish, easy-to-use Web browser for its Mac OS.					
NA	20-02-2017	4.3	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. **CVE ID: CVE-2017-2359**	https://support.apple.com/HT207484	A-APP-SAFAR-030317/08
Transporter Transporter is Apple's Java-based command-line tool to validate metadata and assets and deliver them directly to iTunes.					
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7666**	https://support.apple.com/HT207432	A-APP-TRANS-030317/09
Artifex					
Afpl Ghostscript Ghostscript is a suite of software based on an interpreter for Adobe Systems' PostScript and Portable Document Format (PDF) page description languages.					
Denial of Service	23-02-2017	6.8	Multiple use-after-free vulnerabilities in the gx_image_enum_begin function in base/gxipixel.c in Ghostscript before ecceafe3abba2714ef9b432035fe0739d9b1a283 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document. **CVE ID: CVE-2017-6196**	https://bugs.ghostscript.com/show_bug.cgi?id=697596	A-ART-AFPL-030317/10

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Bilboplanet					
Bilboplanet Bilboplanet - Open-source planet framework blog-agregator in PHP.					
Cross Site Scripting	23-02-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Bilboplanet 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) tribe_name or (2) tags parameter in a tribes page request to user/ or the (3) user_id or (4) fullname parameter to signup.php. **CVE ID: CVE-2014-9916**	NA	A-BIL-BILBO-030317/11
Cisco					
Identity Services Engine Software Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches.					
SQL Injection	21-02-2017	6.5	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). **CVE ID: CVE-2017-3835**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ise	A-CIS-IDENT-030317/12
Intrusion Prevention System Device Manager The Cisco IPS Device Manager (IDM) is a tool that enables you to configure and manage a single Cisco network sensor.					
Gain Information	21-02-2017	5	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. **CVE ID: CVE-2017-3842**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-idm	A-CIS-INTRU-030317/13
Meeting Server Cisco Meeting Server brings premises-based video, audio, and web communication together to meet the collaboration needs of the modern workplace.					
Denial of	21-02-2017	5	A vulnerability in an internal API	https://too	A-CIS-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Service			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. **CVE ID: CVE-2017-3830**	ls.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cms	MEETI-030317/14
Denial of Service	21-02-2017	5.5	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 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. **CVE ID: CVE-2017-3837**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cms1	A-CIS-MEETI-030317/15
Prime Collaboration Assurance Cisco Prime Collaboration is a comprehensive video and voice service assurance and management system with a set of monitoring, troubleshooting, and reporting capabilities that help ensure end users receive a consistent, high-quality video and voice collaboration experience.					
NA	21-02-2017	4	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:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-PRIME-030317/16

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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). **CVE ID: CVE-2017-3844**	sa-20170215-pcp2	
NA	21-02-2017	4	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). **CVE ID: CVE-2017-3843**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp1	A-CIS-PRIME-030317/17
Cross Site Scripting	21-02-2017	4.3	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). **CVE ID: CVE-2017-3845**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp3	A-CIS-PRIME-030317/18
Secure Access Control System Cisco Secure Access Control System ties together an enterprise's network access policy and identity strategy.					
NA	21-02-2017	4	An XML External Entity vulnerability in the web-based user interface of the Cisco Secure Access Control System (ACS) could allow an unauthenticated, remote attacker to have read access to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvi	A-CIS-SECUR-030317/19

			part of the information stored in the affected system. More Information: CSCvc04845. Known Affected Releases: 5.8(2.5). **CVE ID: CVE-2017-3839**	sory/cisco-sa-20170215-acs1	
Cross Site Scripting	21-02-2017	4.3	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). **CVE ID: CVE-2017-3838**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs	A-CIS-SECUR-030317/20
Gain Information	21-02-2017	5	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). **CVE ID: CVE-2017-3841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs3	A-CIS-SECUR-030317/21
NA	21-02-2017	5.8	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). **CVE ID: CVE-2017-3840**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs2	A-CIS-SECUR-030317/22
Unified Communications Manager As the core of the Cisco Collaboration portfolio infrastructure, Cisco Unified Communications Manager is a unified communications call control platform that can deliver the right experience to the right endpoint.					
Gain Information	21-02-2017	4	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:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-UNIFI-030317/23

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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). **CVE ID: CVE-2017-3836**	sa-20170215-cucm3	
Cross Site Scripting	21-02-2017	4.3	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). **CVE ID: CVE-2017-3833**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ucm	A-CIS-UNIFI-030317/24
Cross Site Scripting	21-02-2017	4.3	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)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm2	A-CIS-UNIFI-030317/25

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			12.0(0.98000.422)
			12.0(0.98000.541)
			12.0(0.98000.6).
			CVE ID: CVE-2017-3829		

Cross Site Scripting	21-02-2017	4.3	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). **CVE ID: CVE-2017-3828**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm1	A-CIS-UNIFI-030317/26
Cross Site Scripting	21-02-2017	4.3	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). **CVE ID: CVE-2017-3821**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-cucm	A-CIS-UNIFI-030317/27
Xenserver Citrix XenServer is a server virtualization platform based on the Xen hypervisor that allows IT administrators to host, deploy and manage virtual machines.					
Gain Privileges	16-02-2017	3.7	The (1) ioport_read and (2) ioport_write functions in Xen, when qemu is used as a device	http://xenbits.xen.org/xsa/advis	A-CIT-XENSE-030317/28

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			model within Xen, might allow local x86 HVM guest OS administrators to gain qemu process privileges via vectors involving an out-of-range ioport access. **CVE ID: CVE-2016-9637**	ory-199.html	
Cmsmadesimple					
Cms Made Simple;Form Builder CMS Made Simple (CMSMS) is a free, open source (GPL) content management system (CMS) to provide developers, programmers and site owners a web-based development and administration area; The form builder element can be used to accept payments from donations, sell products online, or any other general accepting of money online.					
Gain Information	21-02-2017	5	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via defaultadmin. **CVE ID: CVE-2017-6072**	NA	A-CMS-CMSM-030317/29
Gain Information	21-02-2017	5	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via exportxml. **CVE ID: CVE-2017-6071**	NA	A-CMS-CMSM-030317/30
Execute Code; Gain Information	21-02-2017	7.5	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. **CVE ID: CVE-2017-6070**	NA	A-CMS-CMSM-030317/31
Disksavvy					
Disksavvy Enterprise DiskSavvy is a disk space usage analyzer capable of analyzing disks, network shares, NAS devices and enterprise storage systems.					
Execute Code Overflow	22-02-2017	7.5	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. **CVE ID: CVE-2017-6187**	NA	A-DIS-DISKS-030317/32
Dotcms					
Dotcms dotCMS is an open source content management system (CMS) for managing content and content					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

driven sites and applications.					
SQL Injection	17-02-2017	7.5	An issue was discovered in dotCMS through 3.6.1. The findChildrenByFilter() function which is called by the web accessible path /categoriesServlet performs string interpolation and direct SQL query execution. SQL quote escaping and a keyword blacklist were implemented in a new class, SQLUtil (main/java/com/dotmarketing/common/util/SQLUtil.java), as part of the remediation of CVE ID: CVE-2016-8902; however, these can be overcome in the case of the q and inode parameters to the /categoriesServlet path. Overcoming these controls permits a number of blind boolean SQL injection vectors in either parameter. The /categoriesServlet web path can be accessed remotely and without authentication in a default dotCMS deployment. **CVE ID: CVE-2017-5344**	NA	A-DOT-DOTCM-030317/33
Dovecot					
Dovecot Dovecot is an open-source IMAP and POP3 server for Linux/UNIX-like systems, written primarily with security in mind.					
Denial of Service	16-02-2017	4.3	The auth component in Dovecot before 2.2.27, when auth-policy is configured, allows a remote attacker to cause a denial of service (crash) by aborting authentication without setting a username. **CVE ID: CVE-2016-8652**	NA	A-DOV-DOVEC-030317/34
F5					
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Analytics;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Domain Name System;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Websafe BIG-IP System is a blend of software and hardware gives you the ability to control the traffic that					

passes through your network. F5's BIG-IP product family comprises purpose-built hardware, modularized software, and virtualized solutions that run the F5 TMOS operating system.					
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-6249**	https://support.f5.com/csp/article/K12685114	A-F5-BIG-I-030317/35
Facebook					
Hhvm HHVM is an open-source virtual machine designed for executing programs written in Hack and PHP.					
NA	17-02-2017	7.5	Infinite recursion in wddx in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2016-6875**	https://github.com/facebook/hhvm/commit/1888810e77b446a79a7674784d5f139fcfa605e2	A-FAC-HHVM-030317/36
Hhvm HHVM is an open-source virtual machine designed for executing programs written in Hack and PHP.					
NA	17-02-2017	7.5	The array_*_recursive functions in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors, related to recursion. **CVE ID: CVE-2016-6874**	https://github.com/facebook/hhvm/commit/05e706d98f748f609b19d8697e490eaab5007d69	A-FAC-HHVM-030317/37
NA	17-02-2017	7.5	Self recursion in compact in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2016-6873**	https://github.com/facebook/hhvm/commit/e264f04ae825a5d97758130cf8eec99862517e7e	A-FAC-HHVM-030317/38

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Overflow	17-02-2017	7.5	Integer overflow in StringUtil::implode in Facebook HHVM before 3.15.0 allows attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2016-6872**	https://github.com/facebook/hhvm/commit/2c9a8fcc73a151608634d3e712973d192027c271	A-FAC-HHVM-030317/39
Overflow	17-02-2017	7.5	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. **CVE ID: CVE-2016-6871**	https://github.com/facebook/hhvm/commit/c00fc9d3003eb06226b58b6a48555f1456ee2475	A-FAC-HHVM-030317/40
NA	17-02-2017	7.5	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. **CVE ID: CVE-2016-6870**	https://github.com/facebook/hhvm/commit/365abe807cab2d60dc9ec307292a06181f77a9c2	A-FAC-HHVM-030317/41
Faststone					
Maxview FastStone MaxView is a fast, compact and innovative image viewer that supports all major graphic formats.					
Denial of Service	21-02-2017	4.3	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. **CVE ID: CVE-2017-6078**	https://github.com/ilsani/rd/tree/master/security-advisories/faststone/maxview- CVE ID: CVE-2017-6078	A-FAS-MAXVI-030317/42
GNU					
Glibc The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

library.					
Denial of Service	16-02-2017	5	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures. **CVE ID: CVE-2016-5417**	https://sourceware.org/bugzilla/show_bug.cgi?id=19257	A-GNU-GLIBC-030317/43
Libiberty The libiberty library is a collection of subroutines used by various GNU programs.					
Denial of Service	24-02-2017	4.3	The demangle_template_value_parm and do_hpacc_template_literal functions in cplus-dem.c in libiberty allow remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted binary. **CVE ID: CVE-2016-4493**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70926	A-GNU-LIBIB-030317/44
Denial of Service; Overflow	24-02-2017	4.3	Buffer overflow in the do_type function in cplus-dem.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary. **CVE ID: CVE-2016-4492**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70926	A-GNU-LIBIB-030317/45
Denial of Service; Overflow	24-02-2017	4.3	The d_print_comp function in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, which triggers infinite recursion and a buffer overflow, related to a node having "itself as ancestor more than once." **CVE ID: CVE-2016-4491**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70909	A-GNU-LIBIB-030317/46
Denial of Service; Overflow	24-02-2017	4.3	Integer overflow in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to inconsistent use of the long and	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70498	A-GNU-LIBIB-030317/47

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			int types for lengths. **CVE ID: CVE-2016-4490**		
Denial of Service; Overflow	24-02-2017	4.3	Integer overflow in the gnu_special function in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to the "demangling of virtual tables." **CVE ID: CVE-2016-4489**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70492	A-GNU-LIBIB-030317/48
Denial of Service	24-02-2017	4.3	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to "ktypevec." **CVE ID: CVE-2016-4488**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70481	A-GNU-LIBIB-030317/49
Denial of Service	24-02-2017	4.3	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to "btypevec." **CVE ID: CVE-2016-4487**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=70481	A-GNU-LIBIB-030317/50
Execute Code; Overflow	24-02-2017	6.8	Integer overflow in the string_appends function in cplus-dem.c in libiberty allows remote attackers to execute arbitrary code via a crafted executable, which triggers a buffer overflow. **CVE ID: CVE-2016-2226**	https://gcc.gnu.org/bugzilla/show_bug.cgi?id=69687	A-GNU-LIBIB-030317/51
Gomlab					
Gom Player GOM Player is a media player for Windows, developed by the Gretech Corporation of South Korea. Its main features include the ability to play some broken media files and find missing codecs using a codec finder service.					
Denial of Service; Overflow; Memory Corruption	21-02-2017	6.8	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. **CVE ID: CVE-2017-5881**	https://www.exploit-db.com/exploits/41367/	A-GOM-GOMP-030317/52
Google					
Chrome Google Chrome is a freeware web browser developed by Google. It was first released in 2008, for					

Microsoft Windows, and was later ported to Linux, macOS, iOS and Android.					
Bypass	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID: CVE-2017-5027**	https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html	A-GOO-CHROM-030317/53
NA	17-02-2017	4.3	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page. **CVE ID: CVE-2017-5026**	https://crbug.com/634108	A-GOO-CHROM-030317/54
Overflow	17-02-2017	4.3	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. **CVE ID: CVE-2017-5025**	https://crbug.com/643950	A-GOO-CHROM-030317/55
Overflow	17-02-2017	4.3	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. **CVE ID: CVE-2017-5024**	https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html	A-GOO-CHROM-030317/56
NA	17-02-2017	4.3	Type confusion in Histogram 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 potentially exploit a near null dereference via a crafted HTML page.	https://crbug.com/651443	A-GOO-CHROM-030317/57

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2017-5023		
Bypass	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID: CVE-2017-5022**	https://crbug.com/663620	A-GOO-CHROM-030317/58
NA	17-02-2017	4.3	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. **CVE ID: CVE-2017-5021**	https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html	A-GOO-CHROM-030317/59
Execute Code; Cross Site Scripting	17-02-2017	4.3	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page. **CVE ID: CVE-2017-5020**	https://crbug.com/668653	A-GOO-CHROM-030317/60
Cross Site Scripting	17-02-2017	4.3	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. **CVE ID: CVE-2017-5018**	https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html	A-GOO-CHROM-030317/61
Gain Information	17-02-2017	4.3	Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video	https://chromereleases.googleblo	A-GOO-CHROM-030317/62

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			memory, which allowed a remote attacker to possibly extract image fragments on systems with GeForce 8600M graphics chips via a crafted HTML page. **CVE ID: CVE-2017-5017**	g.com/2017/01/stable-channel-update-for-desktop.html	
NA	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page. **CVE ID: CVE-2017-5016**	https://crbug.com/673163	A-GOO-CHROM-030317/63
NA	17-02-2017	4.3	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name. **CVE ID: CVE-2017-5015**	https://crbug.com/673971	A-GOO-CHROM-030317/64
NA	17-02-2017	4.3	Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID: CVE-2017-5013**	https://crbug.com/677716	A-GOO-CHROM-030317/65
Gain Information	17-02-2017	4.3	Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page. **CVE ID: CVE-2017-5011**	https://crbug.com/662859	A-GOO-CHROM-030317/66
Cross Site Scripting	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows	https://crbug.com/66	A-GOO-CHROM-

			and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. **CVE ID: CVE-2017-5010**	3476	030317/67
Cross Site Scripting	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. **CVE ID: CVE-2017-5008**	https://crbug.com/668552	A-GOO-CHROM-030317/68
Cross Site Scripting	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. **CVE ID: CVE-2017-5007**	https://crbug.com/671102	A-GOO-CHROM-030317/69
Cross Site Scripting	17-02-2017	4.3	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. **CVE ID: CVE-2017-5006**	https://crbug.com/673170	A-GOO-CHROM-030317/70
NA	17-02-2017	6.8	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 potentially exploit heap corruption via a crafted HTML page. **CVE ID: CVE-2017-5019**	https://crbug.com/666714	A-GOO-CHROM-030317/71

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Overflow	17-02-2017	6.8	Heap buffer overflow during image processing in Skia 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. **CVE ID: CVE-2017-5014**	https://crbug.com/675332	A-GOO-CHROM-030317/72
Overflow	17-02-2017	6.8	A heap buffer overflow in V8 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 potentially exploit heap corruption via a crafted HTML page. **CVE ID: CVE-2017-5012**	https://crbug.com/681843	A-GOO-CHROM-030317/73
Overflow	17-02-2017	6.8	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID: CVE-2017-5009**	https://crbug.com/667504	A-GOO-CHROM-030317/74
Gpgtools					
Libmacgpg Libmacgpg is an Objective-C framework which makes it easy to communicate with gnupg.					
Execute Code	22-02-2017	7.2	The installPackage function in the installerHelper subcomponent in Libmacgpg in GPG Suite before 2015.06 allows local users to execute arbitrary commands with root privileges via shell metacharacters in the xmlPath argument. **CVE ID: CVE-2014-4677**	https://gpgtools.org/releases/gpgsuite/2015.08/release-notes.html	A-GPG-LIBMA-030317/75
Grails					
Pdf Plugin Pdf plugin allows your Grails application to generate PDFs and send them to the browser by converting existing pages in your application to PDF on the fly.					
NA	27-02-2017	4.3	XML External Entity (XXE)	NA	A-GRA-PDF

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			vulnerability in Grails PDF Plugin 0.6 allows remote attackers to read arbitrary files via a crafted XML document. **CVE ID: CVE-2017-6344**		P-030317/76
Graphicsmagick					
Graphicsmagick GraphicsMagick is the swiss army knife of image processing-comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF.					
Denial of Service	27-02-2017	4.3	The DrawDashPolygon function in magick/render.c in GraphicsMagick before 1.3.24 and the SVG renderer in ImageMagick allow remote attackers to cause a denial of service (infinite loop) by converting a circularly defined SVG file. **CVE ID: CVE-2016-5240**	http://hg.graphicsmagick.org/hg/GraphicsMagick?cmd=changeset;node=ddc999ec896c	A-GRA-GRAPH-030317/77
Html5lib					
Html5lib html5lib is a pure-python library for parsing HTML. It is designed to conform to the WHATWG HTML specification, as is implemented by all major web browsers.					
Cross Site Scripting	22-02-2017	4.3	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. **CVE ID: CVE-2016-9910**	https://github.com/html5lib/html5lib-python/issues/11	A-HTM-HTML5-030317/78
Cross Site Scripting	22-02-2017	4.3	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. **CVE ID: CVE-2016-9909**	https://github.com/html5lib/html5lib-python/issues/11	A-HTM-HTML5-030317/79
IBM					
Dashboard Application Services Hub Dashboard Application Services Hub provides visualization and dashboard services in Jazz for Service					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Management.					
Cross Site Request Forgery	24-02-2017	6.8	IBM Jazz for Service Management 1.1.2.1 and 1.1.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 1998714. **CVE ID: CVE-2016-9975**	http://www.ibm.com/support/docview.wss?uid=swg21998714	A-IBM-DASHB-030317/80
Inotes IBM iNotes (formerly IBM Lotus iNotes) is a web-based email client for IBM Notes.					
Cross Site Scripting	23-02-2017	4.3	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. **CVE ID: CVE-2016-5883**	http://www.ibm.com/support/docview.wss?uid=swg21997010	A-IBM-INOTE-030317/81
Rational Doors Next Generation;Rational Requirements Composer IBM Rational DOORS Next Generation offers a smarter way to manage your requirements that can help your teams reduce development costs by up to 57%, accelerate time to market by up to 20%, and lower cost of quality by up to 69%; IBM Rational Requirements Composer software empowers teams to define, manage and report on requirements in a lifecycle development project.					
Cross Site Scripting	23-02-2017	3.5	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. **CVE ID: CVE-2016-6055**	http://www.ibm.com/support/docview.wss?uid=swg21995515	A-IBM-RATIO-030317/82
Rational Rhapsody Design Manager IBM Rational Rhapsody Design Manager is collaborative design management software that helps design teams and their stakeholders to share, trace, review and manage designs.					
Denial of Service	23-02-2017	7.5	IBM Rhapsody DM 4.0, 5.0 and 6.0 is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when	http://www.ibm.com/support/docview.wss	A-IBM-RATIO-030317/83

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 1997798. **CVE ID: CVE-2016-8974**	?uid=swg21997798	
Resilient IBM Resilient incident response platform helps organizations effectively orchestrate their response.					
Cross Site Scripting	16-02-2017	4.3	IBM Resilient v26.0, v26.1, and v26.2 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#: 213457065. **CVE ID: CVE-2016-6062**	https://www.ibm.com/blogs/psirt/ibm-security-bulletin-ibm-resilient-cross-site-scripting-vulnerability-CVE ID: CVE-2016-6062/	A-IBM-RESIL-030317/84
Tivoli Storage Manager IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. It is the flagship product in the IBM Spectrum Protect (Tivoli Storage Manager) family.					
Execute Code; Overflow	24-02-2017	6	IBM Tivoli Storage Manager Server 7.1 could allow an authenticated user with TSM administrator privileges to cause a buffer overflow using a specially crafted SQL query and execute arbitrary code on the server. IBM Reference #: 1998747. **CVE ID: CVE-2016-8998**	http://www.ibm.com/support/docview.wss?uid=swg21998747	A-IBM-TIVOL-030317/85
Websphere Mq IBM MQ is messaging middleware that simplifies and accelerates the integration of diverse applications and business data across multiple platforms.					
NA	22-02-2017	4	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. **CVE ID: CVE-2016-8986**	http://www.ibm.com/support/docview.wss?uid=swg21998648	A-IBM-WEBSP-030317/86

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

NA	22-02-2017	4	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. **CVE ID: CVE-2016-8915**	http://www.ibm.com/support/docview.wss?uid=swg21998649	A-IBM-WEBSP-030317/87
NA	22-02-2017	4	IBM WebSphere MQ 8.0 could allow an authenticated user to crash the MQ channel due to improper data conversion handling. IBM Reference #: 1998661. **CVE ID: CVE-2016-3013**	http://www.ibm.com/support/docview.wss?uid=swg21998661	A-IBM-WEBSP-030317/88
Denial of Service	24-02-2017	4	IBM WebSphere MQ 8.0 could allow an authenticated user with authority to create a cluster object to cause a denial of service to MQ clustering. IBM Reference #: 1998647. **CVE ID: CVE-2016-9009**	http://www.ibm.com/support/docview.wss?uid=swg21998647	A-IBM-WEBSP-030317/89
Gain Information	22-02-2017	4.3	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. **CVE ID: CVE-2016-3052**	http://www.ibm.com/support/docview.wss?uid=swg21998660	A-IBM-WEBSP-030317/90
Iceni					
Argus Argus accurately converts the majority of PDF document types including financial/report based, newspaper/magazines, books and even structured PDF.					
Execute Code; Overflow	28-02-2017	6.8	An exploitable heap corruption vulnerability exists in the loadTrailer functionality of Iceni Argus version 6.6.05. A specially crafted PDF file can cause a heap corruption resulting in arbitrary code execution. An attacker can send/provide a malicious PDF file to trigger this vulnerability. **CVE ID: CVE-2016-8715**	NA	A-ICE-ARGUS-030317/91
Execute Code;	27-02-2017	9.3	An exploitable heap-based buffer	NA	A-ICE-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Overflow			overflow exists in Iceni Argus. When it attempts to convert a malformed PDF with an object encoded w/ multiple encoding types terminating with an LZW encoded type, an overflow may occur due to a lack of bounds checking by the LZW decoder. This can lead to code execution under the context of the account of the user running it. **CVE ID: CVE-2016-8387**		ARGUS-030317/92
Execute Code; Overflow	27-02-2017	9.3	An exploitable heap-based buffer overflow exists in Iceni Argus. When it attempts to convert a PDF containing a malformed font to XML, the tool will attempt to use a size out of the font to search through a linked list of buffers to return. Due to a signedness issue, a buffer smaller than the requested size will be returned. Later when the tool tries to populate this buffer, the overflow will occur which can lead to code execution under the context of the user running the tool. **CVE ID: CVE-2016-8386**	NA	A-ICE-ARGUS-030317/93
Execute Code; Overflow	27-02-2017	9.3	An exploitable uninitialized variable vulnerability which leads to a stack-based buffer overflow exists in Iceni Argus. When it attempts to convert a malformed PDF to XML a stack variable will be left uninitialized which will later be used to fetch a length that is used in a copy operation. In most cases this will allow an aggressor to write outside the bounds of a stack buffer which is used to contain colors. This can lead to code execution under the context of the account running the tool. **CVE ID: CVE-2016-8385**	NA	A-ICE-ARGUS-030317/94
Execute Code;	28-02-2017	9.3	An exploitable integer-overflow	NA	A-ICE-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Overflow			vulnerability exists within Iceni Argus. When it attempts to convert a malformed PDF to XML, it will attempt to convert each character from a font into a polygon and then attempt to rasterize these shapes. As the application attempts to iterate through the rows and initializing the polygon shape in the buffer, it will write outside of the bounds of said buffer. This can lead to code execution under the context of the account running it. **CVE ID: CVE-2016-8389**		ARGUS-030317/95
NA	28-02-2017	9.3	An exploitable arbitrary heap-overwrite vulnerability exists within Iceni Argus. When it attempts to convert a malformed PDF to XML, it will explicitly trust an index within the specific font object and use it to write the font's name to a single object within an array of objects. **CVE ID: CVE-2016-8388**	NA	A-ICE-ARGUS-030317/96
Icoutils Project					
Icoutils The icoutils are a set of command-line programs for extracting and converting images in Microsoft Windows(R) icon and cursor files.					
Overflow	16-02-2017	4.3	An issue was discovered in icoutils 0.31.1. An out-of-bounds read leading to a buffer overflow was observed in the "simple_vec" function in the "extract.c" source file. This affects icotool. **CVE ID: CVE-2017-6011**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=854054	A-ICO-ICOUT-030317/97
Overflow	16-02-2017	4.3	An issue was discovered in icoutils 0.31.1. A buffer overflow was observed in the "extract_icons" function in the "extract.c" source file. This issue can be triggered by processing a corrupted ico file and will result in an icotool crash. **CVE ID: CVE-2017-6010**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=854054	A-ICO-ICOUT-030317/98
Overflow	16-02-2017	4.3	An issue was discovered in icoutils	https://bug	A-ICO-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			0.31.1. A buffer overflow was observed in the "decode_ne_resource_id" function in the "restable.c" source file. This is happening because the "len" parameter for memcpy is not checked for size and thus becomes a negative integer in the process, resulting in a failed memcpy. This affects wrestool. **CVE ID: CVE-2017-6009**	s.debian.org/cgi-bin/bugreport.cgi?bug=854050	ICOUT-030317/99
Imagemagick					
Imagemagick ImageMagick is a free and open-source software suite for displaying, converting, and editing raster image and vector image files.					
Denial of Service; Overflow	16-02-2017	4.3	Heap-based buffer overflow in the IsPixelGray function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.8 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted image file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9556. **CVE ID: CVE-2016-9773**	NA	A-IMA-IMAGE-030317/100
Denial of Service	27-02-2017	4.3	The ReadVICARImage function in coders/vicar.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted VICAR file. **CVE ID: CVE-2015-8903**	https://bugzilla.redhat.com/show_bug.cgi?id=1195271	A-IMA-IMAGE-030317/101
Denial of Service	27-02-2017	4.3	The ReadBlobByte function in coders/pdb.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted PDB file. **CVE ID: CVE-2015-8902**	https://bugzilla.redhat.com/show_bug.cgi?id=1195269	A-IMA-IMAGE-030317/102
Denial of Service	27-02-2017	4.3	ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted MIFF file. **CVE ID: CVE-2015-8901**	https://bugzilla.redhat.com/show_bug.cgi?id=1195265	A-IMA-IMAGE-030317/103

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service	27-02-2017	4.3	The ReadHDRImage function in coders/hdr.c in ImageMagick 6.x and 7.x allows remote attackers to cause a denial of service (infinite loop) via a crafted HDR file. **CVE ID: CVE-2015-8900**	https://github.com/ImageMagick/ImageMagick/commit/97aa7d7cfd2027f6ba7ce42caf8b798541b9cdc6	A-IMA-IMAGE-030317/104
Intel					
X710 Series Driver; Xl710 Series Driver The Intel Ethernet Controller 10 and 40 Gigabit X710/XL710 family extends Intel Virtualization Technology to networks with hardware optimizations.					
Denial of Service	27-02-2017	6.1	Drivers for the Intel Ethernet Controller X710 and Intel Ethernet Controller XL710 families before version 22.0 are vulnerable to a denial of service in certain layer 2 network configurations. **CVE ID: CVE-2016-8105**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00069&languageid=en-fr	A-INT-X710-030317/105
Intersect Alliance					
Snare Epilog Snare Enterprise Epilog for UNIX provides a method to collect any text based log files on the Linux and Solaris operating systems.					
Cross Site Scripting	17-02-2017	3.5	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" action. **CVE ID: CVE-2017-5998**	http://arthrocyber.com/research	A-INT-SNARE-030317/106
Inverse-inc					
Sogo Sogo is a very fast and scalable modern collaboration suite (groupware).					
Gain Information	17-02-2017	4	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	https://github.com/inverse-inc/sogo/commit/717	A-INV-SOGO-030317/107

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			sensitive information about appointments with the "View the Date & Time" restriction, as demonstrated by correlating UIDs and DTSTAMPs between all users. **CVE ID: CVE-2016-6190**	f45f640a2866b76a8984139391fae64339225	
Gain Information	17-02-2017	4	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. **CVE ID: CVE-2016-6189**	https://github.com/inverse-inc/sogo/commit/717f45f640a2866b76a8984139391fae64339225	A-INV-SOGO-030317/108
Cross Site Scripting	17-02-2017	4.3	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. **CVE ID: CVE-2016-6191**	https://sogo.nu/bugs/view.php?id=3718	A-INV-SOGO-030317/109
Cross Site Scripting	17-02-2017	4.3	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. **CVE ID: CVE-2014-9905**	https://github.com/inverse-inc/sogo/commit/c94595ea7f0f843c2d7abf25df039b2bbe707625	A-INV-SOGO-030317/110
Justsystems					
Ichitaro Ichitaro is a Japanese word processor produced by JustSystems, a Japanese software company.					
Execute Code; Overflow	24-02-2017	6.8	JustSystems Ichitaro 2016 Trial contains a vulnerability that exists when trying to open a specially crafted PowerPoint file. Due to the application incorrectly handling the error case for a function's result, the application will use this result in a pointer calculation for reading file data into. Due to this,	NA	A-JUS-ICHIT-030317/111

			the application will read data from the file into an invalid address thus corrupting memory. Under the right conditions, this can lead to code execution under the context of the application. **CVE ID: CVE-2017-2791**		
Cross Site Scripting	24-02-2017	7.5	When processing a record type of 0x3c from a Workbook stream from an Excel file (.xls), JustSystems Ichitaro Office trusts that the size is greater than zero, subtracts one from the length, and uses this result as the size for a memcpy. This results in a heap-based buffer overflow and can lead to code execution under the context of the application. **CVE ID: CVE-2017-2790**	NA	A-JUS-ICHIT-030317/112
Cross Site Scripting	24-02-2017	7.5	When copying filedata into a buffer, JustSystems Ichitaro Office 2016 Trial will calculate two values to determine how much data to copy from the document. If both of these values are larger than the size of the buffer, the application will choose the smaller of the two and trust it to copy data from the file. This value is larger than the buffer size, which leads to a heap-based buffer overflow. This overflow corrupts an offset in the heap used in pointer arithmetic for writing data and can lead to code execution under the context of the application. **CVE ID: CVE-2017-2789**	NA	A-JUS-ICHIT-030317/113
Kodi					
Kodi Kodi is a free and open-source media player software application developed by the XBMC Foundation, a non-profit technology consortium.					
Directory Traversal.	28-02-2017	5	Directory traversal vulnerability in the Chorus2 2.4.2 add-on for Kodi allows remote attackers to read arbitrary files via a	NA	A-KOD-KODI-030317/114

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			%2E%2E%252e (encoded dot dot slash) in the image path, as demonstrated by image/image%3A%2F%2F%2e%2e%252fetc%252fpasswd. **CVE ID: CVE-2017-5982**		
Libdwarf Project					
Libdwarf Libdwarf is a C library intended to simplify reading (and writing) applications using DWARF2, DWARF3.					
Denial of Service; Overflow	17-02-2017	4.3	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. **CVE ID: CVE-2016-7511**	https://sourceforge.net/p/libdwarf/bugs/3/	A-LIB-LIBDW-030317/115
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-7510**	https://sourceforge.net/p/libdwarf/bugs/4/	A-LIB-LIBDW-030317/116
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5040**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/117
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5037**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/118
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5035**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/119

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5034**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/120
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5033**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/121
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5032**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/122
Denial of Service	17-02-2017	4.3	The print_frame_inst_bytes function in libdwarf before 20160923 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file. **CVE ID: CVE-2016-5031**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/123
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5030**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/124
Denial of Service	17-02-2017	4.3	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. **CVE ID: CVE-2016-5029**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/125
Denial of Service	17-02-2017	4.3	The print_frame_inst_bytes function in libdwarf before 20160923 allows remote	https://www.prevanders.net/dwa	A-LIB-LIBDW-030317/126

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			attackers to cause a denial of service (NULL pointer dereference) via an object file with empty bss-like sections. **CVE ID: CVE-2016-5028**	rfbug.html	
Denial of Service	24-02-2017	4.3	dwarf_form.c in libdwarf 20160115 allows remote attackers to cause a denial of service (crash) via a crafted elf file. **CVE ID: CVE-2016-5027**	https://bugzilla.redhat.com/show_bug.cgi?id=1330237	A-LIB-LIBDW-030317/127
Denial of Service	17-02-2017	5	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. **CVE ID: CVE-2016-5044**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/128
Denial of Service	17-02-2017	5	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. **CVE ID: CVE-2016-5043**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/129
Denial of Service	17-02-2017	5	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. **CVE ID: CVE-2016-5042**	https://bugzilla.redhat.com/show_bug.cgi?id=1332145	A-LIB-LIBDW-030317/130
Denial of Service	17-02-2017	5	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. **CVE ID: CVE-2016-5039**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/131
Denial of Service	17-02-2017	5	The dwarf_get_macro_startend_file function in 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. **CVE ID: CVE-2016-5038**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/132

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service	17-02-2017	5	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. **CVE ID: CVE-2016-5036**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/133
Overflow	28-02-2017	7.5	(1) libdwarf/dwarf_leb.c and (2) dwarfdump/print_frames.c in libdwarf before 20161124 allow remote attackers to have unspecified impact via a crafted bit pattern in a signed leb number, aka a "negation overflow." **CVE ID: CVE-2016-9558**	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-030317/134
Libming					
Libming Ming is a library for generating Macromedia Flash files (.swf), written in C, and includes useful utilities for working with .swf files.					
Denial of Service	16-02-2017	4.3	The dumpBuffer function in read.c in the listswf tool in libming 0.4.7 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted SWF file. **CVE ID: CVE-2016-9828**	NA	A-LIB-LIBMI-030317/135
Denial of Service; Overflow	16-02-2017	4.3	The _iprintf function in outputtxt.c in the listswf tool in libming 0.4.7 allows remote attackers to cause a denial of service (buffer over-read) via a crafted SWF file. **CVE ID: CVE-2016-9827**	NA	A-LIB-LIBMI-030317/136
Overflow	16-02-2017	6.8	Heap-based buffer overflow in the parseSWF_RGBA function in parser.c in the listswf tool in libming 0.4.7 allows remote attackers to have unspecified impact via a crafted SWF file. **CVE ID: CVE-2016-9831**	NA	A-LIB-LIBMI-030317/137
Overflow	16-02-2017	6.8	Heap-based buffer overflow in the parseSWF_DEFINEFONT function in parser.c in the listswf tool in libming 0.4.7 allows remote attackers to have unspecified impact via a crafted SWF file.	NA	A-LIB-LIBMI-030317/138

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2016-9829		
Mail-masta					
Mail-masta Plugin Mail-masta Plugin is a newsletter plugin that is full featured, beautiful and simple to use.					
SQL Injection	21-02-2017	6.5	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. **CVE ID: CVE-2017-6098**	https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin	A-MAI-MAIL--030317/139
SQL Injection	21-02-2017	6.5	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. **CVE ID: CVE-2017-6097**	https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin	A-MAI-MAIL--030317/140
SQL Injection	21-02-2017	6.5	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. **CVE ID: CVE-2017-6096**	https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin	A-MAI-MAIL--030317/141
SQL Injection	21-02-2017	7.5	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. **CVE ID: CVE-2017-6095**	https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin	A-MAI-MAIL--030317/142
Mantisbt					
Mantisbt MantisBT is a popular free web-based bug tracking system.					
Cross Site Scripting	17-02-2017	2.6	MantisBT before 1.3.1 and 2.x before 2.0.0-beta.2 uses a weak Content Security Policy when	https://mantisbt.org/bugs/view.	A-MAN-MANTI-030317/143

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			using the Gravatar plugin, which allows remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors. **CVE ID: CVE-2016-7111**	php?id=21263	
Cross Site Scripting	17-02-2017	4.3	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. **CVE ID: CVE-2016-5364**	https://mantisbt.org/bugs/view.php?id=20956	A-MAN-MANTI-030317/144
Metalgenix					
Genixcms GeniXCMS is a PHP Based Content Management System and Framework (CMSF).					
Execute Code; SQL Injection	17-02-2017	6.5	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. **CVE ID: CVE-2017-6065**	https://github.com/semplon/GeniXCMS/issues/71	A-MET-GENIX-030317/145
Bypass; Cross Site Request Forgery	21-02-2017	7.5	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. **CVE ID: CVE-2017-5959**	https://github.com/semplon/GeniXCMS/releases/tag/v1.0.2	A-MET-GENIX-030317/146
Microsoft					
Edge;Internet Explorer Microsoft Edge (codename "Spartan") is a web browser developed by Microsoft and included in Windows 10, Windows 10 Mobile, Xbox One, and Windows Holographic; Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.					
Execute Code	26-02-2017	7.6	Microsoft Internet Explorer 11 and Microsoft Edge have a type confusion issue in the Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement function in mshtml.dll, which allows remote attackers to execute arbitrary code via vectors involving a	NA	A-MIC-EDGE;-030317/147

			crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element. **CVE ID: CVE-2017-0037**		
Munin-monitoring					
Munin Munin is a free and open-source computer system monitoring, network monitoring and infrastructure monitoring software application.					
NA	22-02-2017	1.9	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. **CVE ID: CVE-2017-6188**	https://www.debian.org/security/2017/dsa-3794	A-MUN-MUNIN-030317/148
Opentext					
Documentum Content Server Documentum Content Server is a platform that manages content in a repository consisting of three parts: a content server, a relational database, and a place to store files.					
Execute Code; SQL Injection	22-02-2017	6.5	OpenText Documentum Content Server (formerly EMC Documentum Content Server) 7.3, when PostgreSQL Database is used and return_top_results_row_based config option is false, does not properly restrict DQL hints, which allows remote authenticated users to conduct DQL injection attacks and execute arbitrary DML or DDL commands via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-2520. **CVE ID: CVE-2017-5585**	NA	A-OPE-DOCUM-030317/149
Documentum D2 OpenText Documentum D2 is the advanced, intuitive, and configurable content-centric client for Documentum that accelerates adoption of OpenText applications.					
Execute Code	22-02-2017	7.5	OpenText Documentum D2 (formerly EMC Documentum D2) 4.x allows remote attackers to execute arbitrary commands via a crafted serialized Java object,	NA	A-OPE-DOCUM-030317/150

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			related to the BeanShell (bsh) and Apache Commons Collections (ACC) libraries. **CVE ID: CVE-2017-5586**		
Otrs					
Otrs OTRS is one of the most flexible web-based ticketing systems used for Customer Service, Help Desk, IT Service Management.					
Cross Site Scripting	16-02-2017	4.3	Cross-site scripting (XSS) vulnerability in Open Ticket Request System (OTRS) 3.3.x before 3.3.16, 4.0.x before 4.0.19, and 5.0.x before 5.0.14 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment. **CVE ID: CVE-2016-9139**	https://www.otrs.com/security-advisory-2016-02-security-update-otrs/	A-OTR-OTRS-030317/151
Paypal					
Merchant-sdk-php merchant-sdk-php - PHP SDK for integrating with PayPal's Express Checkout / MassPay / Web Payments Pro APIs.					
Cross Site Scripting	23-02-2017	4.3	Cross-site scripting (XSS) vulnerability in GetAuthDetails.html.php in PayPal PHP Merchant SDK (aka merchant-sdk-php) 3.9.1 allows remote attackers to inject arbitrary web script or HTML via the token parameter. **CVE ID: CVE-2017-6099**	NA	A-PAY-MERCH-030317/152
Plone					
Plone Plone is a free and open source content management system built on top of the Zope application server.					
Bypass	24-02-2017	3.5	Chameleon (five.pt) in Plone 5.0rc1 through 5.1a1 allows remote authenticated users to bypass Restricted Python by leveraging permissions to create or edit templates. **CVE ID: CVE-2016-4043**	https://plone.org/security/hotfix/20160419/bypass-restricted-python	A-PLO-PLONE-030317/153
Gain Information	24-02-2017	5	Plone 3.3 through 5.1a1 allows remote attackers to obtain information about the ID of sensitive content via unspecified	https://plone.org/security/hotfix/20160419/	A-PLO-PLONE-030317/154

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			vectors. **CVE ID: CVE-2016-4042**	unauthorized-disclosure-of-site-content	
NA	24-02-2017	7.5	Plone 4.0 through 5.1a1 does not have security declarations for Dexterity content-related WebDAV requests, which allows remote attackers to gain webdav access via unspecified vectors. **CVE ID: CVE-2016-4041**	https://plone.org/security/hotfix/20160419/privilege-escalation-in-webdav	A-PLO-PLONE-030317/155
Qemu					
Qemu QEMU is a generic and open source machine emulator and virtualizer.					
Denial of Service	27-02-2017	2.1	The virtio_gpu_set_scanout function in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a scanout id in a VIRTIO_GPU_CMD_SET_SCANOUT command larger than num_scanouts. **CVE ID: CVE-2016-10029**	http://git.qemu-project.org/?p=qemu.git;a=commit;h=2fe760554eb3769d70f608a158474f	A-QEM-QEMU-030317/156
Denial of Service	27-02-2017	2.1	The virgl_cmd_get_capset function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a VIRTIO_GPU_CMD_GET_CAPSET command with a maximum capabilities size with a value of 0. **CVE ID: CVE-2016-10028**	http://git.qemu-project.org/?p=qemu.git;a=commit;h=abd7f08b2353f43274b785db8c7224f082ef4d31	A-QEM-QEMU-030317/157
Radare					
Radare2 radare2 - unix-like reverse engineering framework and commandline tools.					
Denial of Service	23-02-2017	4.3	The r_read_* functions in libr/include/r_endian.h in radare2 1.2.1 allow remote attackers to	https://github.com/radare/radar	A-RAD-RADAR-030317/158

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by the r_read_le32 function. **CVE ID: CVE-2017-6197**	e2/issues/6816	
Rubyzip					
Rubyzip rubyzip is a ruby module for reading and writing zip files.					
Directory Traversal	27-02-2017	7.5	The Zip::File component in the rubyzip gem before 1.2.1 for Ruby has a directory traversal vulnerability. If a site allows uploading of .zip files, an attacker can upload a malicious file that uses "../" pathname substrings to write arbitrary files to the filesystem. **CVE ID: CVE-2017-5946**	https://github.com/rubyzip/rubyzip/releases	A-RUB-RUBYZ-030317/159
Shadow Project					
Shadow The Shadow Project is an open source project aiming to be the core of privacy, where people will build decentralized applications.					
Overflow; Gain Privileges	17-02-2017	4.6	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap. **CVE ID: CVE-2016-6252**	https://github.com/shadow-maint/shadow/issues/27	A-SHA-SHADO-030317/160
Siemens					
Ruggedcom Network Management Software Ruggedcom NMS is fully-featured enterprise grade network management software based on the OpenNMS platform.					
Cross Site Scripting	27-02-2017	4.3	A non-privileged user of the Siemens web application RUGGEDCOM NMS < V1.2 on port 8080/TCP and 8081/TCP could perform a persistent Cross-Site Scripting (XSS) attack, potentially resulting in obtaining administrative permissions. **CVE ID: CVE-2017-2683**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-363881.pdf	A-SIE-RUGGE-030317/161
Simplesamlphp					
Simplesamlphp SimpleSAMLphp is an award-winning application written in native PHP that deals with					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

authentication.					
Denial of Service	16-02-2017	4	The SimpleSAML_XML_Validator class constructor in SimpleSAMLphp before 1.14.11 might allow remote attackers to spoof signatures on SAML 1 responses or possibly cause a denial of service (memory consumption) by leveraging improper conversion of return values to boolean. **CVE ID: CVE-2016-9955**	https://simplesamlphp.org/security/201612-02	A-SIM-SIMPL-030317/162
Tcpdf Project					
Tcpdf TCPDF is a PHP class for generating PDF documents without requiring external extensions.					
NA	23-02-2017	5	tcpdf before 6.2.0 uploads files from the server generating PDF-files to an external FTP. **CVE ID: CVE-2017-6100**	https://sourceforge.net/p/tcpdf/bugs/1005/	A-TCP-TCPDF-030317/163
Tenable					
Log Correlation Engine Tenable Log Correlation Engine stores, compresses and analyzes any type of ASCII log generated by thousands of network devices and applications.					
Cross Site Scripting	28-02-2017	3.5	Cross-site scripting (XSS) vulnerability in Tenable Log Correlation Engine (aka LCE) before 4.8.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2016-9261**	https://www.tenable.com/security/tns-2016-18	A-TEN-LOGC-030317/164
Nessus Nessus is a proprietary vulnerability scanner developed by Tenable Network Security.					
Cross Site Scripting	28-02-2017	3.5	Cross-site scripting (XSS) vulnerability in Tenable Nessus before 6.9.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2016-9259**	https://www.tenable.com/security/tns-2016-17	A-TEN-NESSU-030317/165
Tigervnc					
Tigervnc TigerVNC is a high-performance, platform-neutral implementation of VNC (Virtual Network Computing), a client/server application that allows users to launch and interact with graphical					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

applications on remote machines.					
Execute Code; Overflow	28-02-2017	6.8	Buffer overflow in the ModifiablePixelBuffer::fillRect function in TigerVNC before 1.7.1 allows remote servers to execute arbitrary code via an RRE message with subrectangle outside framebuffer boundaries. **CVE ID: CVE-2017-5581**	https://github.com/TigerVNC/tigervnc/releases/tag/v1.7.1	A-TIG-TIGER-030317/166
Tnef Project					
Tnef Transport Neutral Encapsulation Format or TNEF is a proprietary email attachment format used by Microsoft Outlook and Microsoft Exchange Server.					
NA	23-02-2017	6.8	An issue was discovered in tnef before 1.4.13. Four 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. **CVE ID: CVE-2017-6310**	NA	A-TNE-TNEF-030317/167
NA	23-02-2017	6.8	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. **CVE ID: CVE-2017-6309**	NA	A-TNE-TNEF-030317/168
Overflow	23-02-2017	6.8	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. **CVE ID: CVE-2017-6308**	NA	A-TNE-TNEF-030317/169
NA	23-02-2017	6.8	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. **CVE ID: CVE-2017-6307**	NA	A-TNE-TNEF-030317/170

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Trendmicro					
Interscan Web Security Virtual Appliance The InterScan Web Security Virtual Appliance (IWSVA) is a gateway solution, providing protection for web-based threats via HTTP and FTP.					
Cross Site Scripting	21-02-2017	3.5	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. **CVE ID: CVE-2016-9316**	https://success.trendmicro.com/solution/1116672	A-TRE-INTER-030317/171
NA	21-02-2017	4	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. **CVE ID: CVE-2016-9315**	https://success.trendmicro.com/solution/1116672	A-TRE-INTER-030317/172
Gain Information	21-02-2017	4	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	https://success.trendmicro.com/solution/1116672	A-TRE-INTER-030317/173

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			passwd/shadow files, RSA certificates, Private Keys and Default Passphrase, etc. This was resolved in Version 6.5 CP 1737. **CVE ID: CVE-2016-9314**		
Exec Code	21-02-2017	9	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. **CVE ID: CVE-2016-9269**	https://success.trendmicro.com/solution/1116672	A-TRE-INTER-030317/174
Vce Vision					
Intelligent Operations VCE Vision Intelligent Operations offers improved automation, flexibility, and simplicity for converged infrastructures.					
NA	21-02-2017	2.1	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. **CVE ID: CVE-2015-4056**	http://seclists.org/bugtraq/2015/Jun/91	A-VCE-INTEL-030317/175
VIM					
VIM Vim is a highly configurable text editor built to enable efficient text editing.					
Overflow	27-02-2017	7.5	An integer overflow at an unserialize_uep memory allocation site would occur for vim before patch 8.0.0378, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows. **CVE ID: CVE-2017-6350**	NA	A-VIM-VIM-030317/176
Overflow	27-02-2017	7.5	An integer overflow at a u_read_undo memory allocation site would occur for vim before	NA	A-VIM-VIM-030317/177

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			patch 8.0.0377, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows. **CVE ID: CVE-2017-6349**		
Wireshark					
Wireshark Wireshark is a network protocol analyzer for Unix and Windows.					
NA	17-02-2017	7.8	In Wireshark 2.2.4 and earlier, a crafted or malformed STANAG 4607 capture file will cause an infinite loop and memory exhaustion. If the packet size field in a packet header is null, the offset to read from will not advance, causing continuous attempts to read the same zero length packet. This will quickly exhaust all system memory. **CVE ID: CVE-2017-6014**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13416	A-WIR-WIRES-030317/178
Wolfssl					
Wolfssl Wolfssl is a small, portable, embedded SSL/TLS library targeted for use by embedded systems developers.					
Gain Information	23-02-2017	2.1	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. **CVE ID: CVE-2017-6076**	https://github.com/wolfSSL/wolfssl/releases/tag/v3.10.2-stable	A-WOL-WOLFS-030317/179
Wso2					
Carbon WSO2 Carbon is the core platform on which WSO2 middleware products are built. It is based on Java OSGi technology, which allows components to be dynamically installed, started, stopped, updated, and uninstalled, and it eliminates component version conflicts.					
Cross Site Request Forgery	16-02-2017	3.5	Cross-site request forgery (CSRF) vulnerability in WSO2 Carbon 4.4.5 allows remote attackers to hijack the authentication of privileged users for requests that shutdown a server via a shutdown action to server-admin/proxy_ajaxprocessor.jsp.	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2016-0101	A-WSO-CARBO-030317/180

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2016-4315		
Directory Traversal	16-02-2017	4	Directory traversal vulnerability in the LogViewer Admin Service in WSO2 Carbon 4.4.5 allows remote authenticated administrators to read arbitrary files via a .. (dot dot) in the logFile parameter to downloadgz-ajaxprocessor.jsp. **CVE ID: CVE-2016-4314**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2016-0098	A-WSO-CARBO-030317/181
Cross Site Scripting	16-02-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in WSO2 Carbon 4.4.5 allow remote attackers to inject arbitrary web script or HTML via the (1) setName parameter to identity-mgt/challenges-mgt.jsp; the (2) webappType or (3) httpPort parameter to webapp-list/webapp_info.jsp; the (4) dsName or (5) description parameter to ndatasource/newdatasource.jsp; the (6) phase parameter to viewflows/handlers.jsp; or the (7) url parameter to ndatasource/validateconnection-ajaxprocessor.jsp. **CVE ID: CVE-2016-4316**	NA	A-WSO-CARBO-030317/182
Enablement Server For Java WSO2 SOA Enablement Server for Java is a robust enterprise-ready Web services platform.					
Cross Site Scripting	16-02-2017	4.3	Cross-site scripting (XSS) vulnerability in WSO2 SOA Enablement Server for Java/6.6 build SSJ-6.6-20090827-1616 and earlier allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO. **CVE ID: CVE-2016-4327**	NA	A-WSO-ENABL-030317/183
Identity Server WSO2 Identity Server efficiently undertakes the complex task of identity management across enterprise applications, services and APIs.					
Denial of Service	16-02-2017	6	XML external entity (XXE) vulnerability in the XACML flow feature in WSO2 Identity Server 5.1.0 before WSO2-CARBON-	https://docs.wso2.com/display/Security/Secu	A-WSO-IDENT-030317/184

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			PATCH-4.4.0-0231 allows remote authenticated users with access to XACML features to read arbitrary files, cause a denial of service, conduct server-side request forgery (SSRF) attacks, or have unspecified other impact via a crafted XACML request to entitlement/eval-policy-submit.jsp. NOTE: this issue can be combined with CVE-2016-4311 to exploit the vulnerability without credentials. **CVE ID: CVE-2016-4312**	rity+Advisory+WSO2-2016-0096	
Cross Site Request Forgery	16-02-2017	6.8	Cross-site request forgery (CSRF) vulnerability in the XACML flow feature in WSO2 Identity Server 5.1.0 allows remote attackers to hijack the authentication of privileged users for requests that process XACML requests via an entitlement/eval-policy-submit.jsp request. **CVE ID: CVE-2016-4311**	NA	A-WSO-IDENT-030317/185
Ytnef Project					
Ytnef Ytnef is a program to work with procmail to decode TNEF streams (winmail.dat attachments) like those created with Outlook.					
NA	23-02-2017	4.3	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." **CVE ID: CVE-2017-6299**	NA	A-YTN-YTNEF-030317/186
Directory Traversal	23-02-2017	6.8	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." **CVE ID: CVE-2017-6306**	NA	A-YTN-YTNEF-030317/187
NA	23-02-2017	6.8	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."	NA	A-YTN-YTNEF-030317/188

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2017-6305		
NA	23-02-2017	6.8	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." **CVE ID: CVE-2017-6304**	NA	A-YTN-YTNEF-030317/189
Overflow	23-02-2017	6.8	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." **CVE ID: CVE-2017-6303**	NA	A-YTN-YTNEF-030317/190
Overflow	23-02-2017	6.8	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "5 of 9. Integer Overflow." **CVE ID: CVE-2017-6302**	NA	A-YTN-YTNEF-030317/191
NA	23-02-2017	6.8	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." **CVE ID: CVE-2017-6301**	NA	A-YTN-YTNEF-030317/192
Overflow	23-02-2017	6.8	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." **CVE ID: CVE-2017-6300**	NA	A-YTN-YTNEF-030317/193
NA	23-02-2017	6.8	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." **CVE ID: CVE-2017-6298**	NA	A-YTN-YTNEF-030317/194
Zabbix					
Zabbix Zabbix is a mature and effortless enterprise-class open source monitoring solution for network monitoring and application monitoring of millions of metrics.					
Execute Code; SQL Injection	16-02-2017	7.5	SQL injection vulnerability in Zabbix before 2.2.14 and 3.0 before 3.0.4 allows remote attackers to execute arbitrary SQL commands via the toggle_ids array parameter in latest.php. **CVE ID: CVE-2016-10134**	https://support.zabbix.com/browse/ZBX-11023	A-ZAB-ZABBI-030317/195

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Application; Operating System (A/OS)

Apple/Apple

Apple Tv/Icloud;Itunes;Safari

Apple TV (stylized as tv) is a digital media player and a microconsole developed and sold by Apple Inc/ iCloud makes sure you always have the latest versions of your most important things — documents, photos, notes, contacts, and more — on all your devices; iTunes is the world's best way to play — and add to — your collection of music, movies, TV shows, apps, audiobooks, and more. Right on your Mac or PC; Safari is a web browser developed by Apple based on the WebKit engine.

Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-4613**	https://support.apple.com/HT207273	A-OS-APP-APPLE-030317/196

Apple Tv;Iphone Os/Icloud;Itunes;Safari

Apple TV (stylized as tv) is a digital media player and a microconsole developed and sold by Apple Inc; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. / iCloud makes sure you always have the latest versions of your most important things — documents, photos, notes, contacts, and more — on all your devices; iTunes is the world's best way to play — and add to — your collection of music, movies, TV shows, apps, audiobooks, and more. Right on your Mac or PC; Safari is a web browser developed by Apple based on the WebKit engine.

Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2356**	https://support.apple.com/HT207481	A-OS-APP-APPLE-030317/197

Apple Tv;Iphone Os/Icloud;Itunes;Safari

Apple TV (stylized as tv) is a digital media player and a microconsole developed and sold by Apple Inc; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. / iCloud makes sure you always have the latest versions of your most important things — documents, photos, notes, contacts, and more — on all your devices; iTunes is the world's best way to play — and add to

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

— your collection of music, movies, TV shows, apps, audiobooks, and more. Right on your Mac or PC; Safari is a web browser developed by Apple based on the WebKit engine.					
Denial of Service; Execute Code; Overflow	20-02-2017	6.8	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. **CVE ID: CVE-2017-2355**	https://support.apple.com/HT207481	A-OS-APP-APPLE-030317/198
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2354**	https://support.apple.com/HT207481	A-OS-APP-APPLE-030317/199
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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" 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. **CVE ID: CVE-2016-7578**	https://support.apple.com/HT207274	A-OS-APP-APPLE-030317/200
Denial of Service;	20-02-2017	6.8	An issue was discovered in certain Apple products. iOS before 10 is	https://support.apple.c	A-OS-APP-APPLE-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Execute Code; Overflow; Memory Corruption			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. **CVE ID: CVE-2016-4764**	om/HT207 143	030317/201
Bypass; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2017-2365**	https://support.apple.com/HT207482	A-OS-APP-APPLE-030317/202
Bypass; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2017-2350**	https://support.apple.com/HT207484	A-OS-APP-APPLE-030317/203
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2373**	https://support.apple.com/HT207482	A-OS-APP-APPLE-030317/204

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2369**	https://support.apple.com/HT207482	A-OS-APP-APPLE-030317/205
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2017-2362**	https://support.apple.com/HT207482	A-OS-APP-APPLE-030317/206
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-4677**	https://support.apple.com/HT207272	A-OS-APP-APPLE-030317/207
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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	https://support.apple.com/HT207272	A-OS-APP-APPLE-030317/208

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			web site. **CVE ID: CVE-2016-4666**		
Apple Tv;Iphone Os;Watch Os/Safari Apple TV (stylized as tv) is a digital media player and a microconsole developed and sold by Apple Inc; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc. /Safari is a web browser developed by Apple based on the WebKit engine.					
Bypass; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2017-2363**	https://support.apple.com/HT207482	A-OS-APP-APPLE-030317/209
Icloud;Itunes;Safari/Iphone Os iCloud makes sure you always have the latest versions of your most important things — documents, photos, notes, contacts, and more — on all your devices; iTunes is the world's best way to play — and add to — your collection of music, movies, TV shows, apps, audiobooks, and more. Right on your Mac or PC; Safari is a web browser developed by Apple based on the WebKit engine/ iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc.					
Bypass; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7599**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/210
Gain Information	20-02-2017	4.3	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	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/211

			process memory via a crafted web site. **CVE ID: CVE-2016-7598**		
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7592**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/212
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7586**	https://support.apple.com/HT207427	A-OS-APP-ICLOU-030317/213
DoS Overflow Mem. Corr. +Info	20-02-2017	5.8	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. **CVE ID: CVE-2016-4743**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/214
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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 "WebKit" component. It allows	https://support.apple.com/HT207481	A-OS-APP-ICLOU-030317/215

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2366**		
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7656**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/216
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7654**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/217
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7652**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/218

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7649**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/219
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7648**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/220
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7646**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/221
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/222

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2016-7645**		
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7642**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/223
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7641**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/224
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7640**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/225

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7639**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/226
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7635**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/227
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7632**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/228
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/229

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2016-7611**		
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7610**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/230
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7587**	https://support.apple.com/HT207427	A-OS-APP-ICLOU-030317/231
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-4692**	https://support.apple.com/HT207422	A-OS-APP-ICLOU-030317/232

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Icloud;Itunes;Safari/Iphone Os;Watch Os iCloud makes sure you always have the latest versions of your most important things — documents, photos, notes, contacts, and more — on all your devices; iTunes is the world's best way to play — and add to — your collection of music, movies, TV shows, apps, audiobooks, and more. Right on your Mac or PC; Safari is a web browser developed by Apple based on the WebKit engine/ iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc/ watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7589**	https://support.apple.com/HT207421	A-OS-APP-ICLOU-030317/233
Iphone Os/Safari iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc/Safari is a web browser developed by Apple based on the WebKit engine.					
Cross Site Scripting	20-02-2017	2.6	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. **CVE ID: CVE-2016-7650**	https://support.apple.com/HT207422	A-OS-APP-IPHON-030317/234
Bypass; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2017-2364**	https://support.apple.com/HT207482	A-OS-APP-IPHON-030317/235
Gain Information	20-02-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is	https://support.apple.com/HT207	A-OS-APP-IPHON-030317/236

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a blob URL on a web site. **CVE ID: CVE-2016-7623**	422	
Iphone Os;Mac Os X;Watch Os/Safari iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers ("Macs"), having been preinstalled on all Macs since 2002; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc/ Safari is a web browser developed by Apple based on the WebKit engine.					
Execute Code	20-02-2017	9.3	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. **CVE ID: CVE-2016-7613**	https://support.apple.com/HT207270	A-OS-APP-IPHON-030317/237
Ubuntu Linux/Pcsc-lite Ubuntu is a computer operating system based on the Debian Linux distribution and distributed as free and open source software, using its own desktop environment/ PCSC-Lite is an open source implementation of PC/SC, part of a global project named MUSCLE (Movement for the Use of Smart Cards in a Linux Environment).					
Denial of Service	23-02-2017	5	Use-after-free vulnerability in pcsc-lite before 1.8.20 allows a remote attackers to cause denial of service (crash) via a command that uses "cardsList" after the handle has been released through the SCardReleaseContext function. **CVE ID: CVE-2016-10109**	https://anonscm.debian.org/cgit/pcsclite/PCSC.git/commit/?id=697fe05967af7ea215bcd5d5774be587780c9e22	A-OS-CAN-UBUNT-030317/238
Debian Linux/Quagga Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project/ Quagga is a routing software suite, providing implementations of OSPFv2, OSPFv3, RIP v1 and v2, RIPng and BGP-4 for Unix platforms, particularly FreeBSD, Linux, Solaris and NetBSD.					

Overflow	22-02-2017	7.5	It was discovered that the zebra daemon in Quagga before 1.0.20161017 suffered from a stack-based buffer overflow when processing IPv6 Neighbor Discovery messages. The root cause was relying on BUFSIZ to be compatible with a message size; however, BUFSIZ is system-dependent. **CVE ID: CVE-2016-1245**	https://www.debian.org/security/2016/dsa-3695	A-OS-DEB-DEBIA-030317/239
Debian Linux/Fedora/Flightgear Debian is a free operating system (OS) for your computer/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel/ FlightGear Flight Simulator is a free, open source multi-platform flight simulator developed by the FlightGear project since 1997.					
NA	22-02-2017	5	The route manager in FlightGear before 2016.4.4 allows remote attackers to write to arbitrary files via a crafted Nasal script. **CVE ID: CVE-2016-9956**	https://sourceforge.net/projects/flightgear/files/release-2016.4/	A-OS-DEB-DEBIA-030317/240
Fedoraproject/Gnome					
Fedora/Gtk-vnc Fedora (formerly Fedora Core) is an operating system based on the Linux kernel/ gtk-vnc is a VNC viewer widget for GTK.					
Execute Code	28-02-2017	6.8	gtk-vnc before 0.7.0 does not properly check boundaries of subrectangle-containing tiles, which allows remote servers to execute arbitrary code via the src x, y coordinates in a crafted (1) rre, (2) hextile, or (3) copyrect tile. **CVE ID: CVE-2017-5884**	https://bugzilla.gnome.org/show_bug.cgi?id=778048	A-OS-FED-FEDOR-030317/241
Denial of Service; Execute Code; Overflow	28-02-2017	7.5	Multiple integer overflows in the (1) vnc_connection_server_message and (2) vnc_color_map_set functions in gtk-vnc before 0.7.0 allow remote servers to cause a denial of service (crash) or possibly execute arbitrary code via vectors involving SetColorMapEntries, which triggers a buffer overflow. **CVE ID: CVE-2017-5885**	https://bugzilla.gnome.org/show_bug.cgi?id=778050	A-OS-FED-FEDOR-030317/242

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Fedoraproject/GNU					
Fedora/ED Fedora (formerly Fedora Core) is an operating system based on the Linux kernel/ Ed is a line-oriented text editor, used to create, display, and modify text files (both interactively and via shell scripts).					
Denial of Service	16-02-2017	5	regex.c in GNU ed before 1.14.1 allows attackers to cause a denial of service (crash) via a malformed command, which triggers an invalid free. **CVE ID: CVE-2017-5357**	NA	A-OS-FED-FEDOR-030317/243
Fedoraproject/Zend					
Fedora/Zend Framework Fedora (formerly Fedora Core) is an operating system based on the Linux kernel/ gtk-vnc is a VNC viewer widget for GTK.					
SQL Injection	16-02-2017	7.5	The (1) order and (2) group methods in Zend_Db_Select in the Zend Framework before 1.12.19 might allow remote attackers to conduct SQL injection attacks via vectors related to use of the character pattern [\w]* in a regular expression. **CVE ID: CVE-2016-6233**	https://framework.zend.com/security/advisory/ZF2016-02	A-OS-FED-FEDOR-030317/244
SQL Injection	16-02-2017	7.5	The (1) order and (2) group methods in Zend_Db_Select in the Zend Framework before 1.12.20 might allow remote attackers to conduct SQL injection attacks by leveraging failure to remove comments from an SQL statement before validation. **CVE ID: CVE-2016-4861**	https://framework.zend.com/security/advisory/ZF2016-03	A-OS-FED-FEDOR-030317/245
IBM/IBM					
Security Access Manager 9.0 Firmware; Security Access Manager For Web 7.0 Firmware; Security Access Manager For Web 8.0 Firmware / Security Access Manager For Mobile IBM Security Access Manager integrated appliance is designed to manage Access in the world of Hybrid Cloud & enable SSO and identity federation to apps running inside & outside of the enterprise.					
NA	16-02-2017	5	IBM Security Access Manager for Web 7.0.0, 8.0.0, and 9.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM Reference #: 1996868.	http://www.ibm.com/support/docview.wss?uid=swg21996868	A-OS-IBM-SECUR-030317/246

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2016-5919		
Opensuse Project/Tigervnc					
Leap/Tigervnc LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ TigerVNC is VNC server and client software, started as a fork of TightVNC in 2009.					
Denial of Service; Overflow	28-02-2017	5	The Xvnc server in TigerVNC allows remote attackers to cause a denial of service (invalid memory access and crash) by terminating a TLS handshake early. **CVE ID: CVE-2016-10207**	https://bugzilla.suse.com/show_bug.cgi?id=1023012	A-OS-OPE-LEAP/-030317/247
Hardware (H)					
Allwinner;AMD;Intel;Nvidia;Samsung					
A64/Athlon Ii 640 X4;E-350;Fx-8120 8-core;Fx-8320 8-core;Fx-8350 8-core;Phenom 9550 4-core/Atom C2750;Celeron N2840;Core I5 M480;Core I7 920;Core I7-2620qm;Core I7-3632qm;Core I7-4500u;Core I7-6700k;Xeon E3-1240 V5;Xeon E5-2658 V2/Tegra K1 Cd570m-a1;Tegra K1 Cd580m-a1/Exynos 5800 NA					
Gain Information	27-02-2017	5	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of modern ARM processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code pointers from JavaScript, breaking ASLR. **CVE ID: CVE-2017-5927**	NA	H-ALL-A64/A-030317/248
Gain Information	27-02-2017	5	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of modern AMD processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code pointers from JavaScript, breaking ASLR. **CVE ID: CVE-2017-5926**	NA	H-ALL-A64/A-030317/249
Gain Information	27-02-2017	5	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of	NA	H-ALL-A64/A-030317/250

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			modern Intel processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code pointers from JavaScript, breaking ASLR. **CVE ID: CVE-2017-5925**		
Operating System (OS)					
Apple					
Apple Tv;Iphone Os;Mac Os X Apple TV gives you access to everything you want to see and hear — like movies, music, photos, games, news and sports; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers.					
Gain Information	20-02-2017	4.3	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 a proxy password authentication requirement and obtain sensitive information. **CVE ID: CVE-2016-7579**	https://support.apple.com/HT207271	O-APP-APPLE-030317/251
Apple Tv;Iphone Os;Mac Os X;Watch Os Apple TV gives you access to everything you want to see and hear — like movies, music, photos, games, news and sports; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
NA	20-02-2017	4.3	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.	https://support.apple.com/HT207270	O-APP-APPLE-030317/252

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CVE ID: CVE-2016-4679		
Denial of Service; Gain Information	20-02-2017	5.8	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. **CVE ID: CVE-2016-4660**	https://support.apple.com/HT207275	O-APP-APPLE-030317/253
NA	20-02-2017	6.8	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. **CVE ID: CVE-2016-7584**	https://support.apple.com/HT207275	O-APP-APPLE-030317/254
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-4673**	https://support.apple.com/HT207270	O-APP-APPLE-030317/255
Denial of Service; Execute Code	20-02-2017	7.2	An issue was discovered in certain Apple products. iOS before 10.1 is affected. macOS	https://support.apple.com/HT207	O-APP-APPLE-030317/256

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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. **CVE ID: CVE-2016-4669**	270	
Denial of Service; Execute Code; Overflow	20-02-2017	9.3	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. **CVE ID: CVE-2017-2370**	https://support.apple.com/HT207487	O-APP-APPLE-030317/257
Denial of Service; Execute Code	20-02-2017	9.3	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. **CVE ID: CVE-2017-2360**	https://support.apple.com/HT207487	O-APP-APPLE-030317/258
Execute Code	20-02-2017	9.3	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	https://support.apple.com/HT207270	O-APP-APPLE-030317/259

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

		🟥	privileged context via a crafted app. **CVE ID: CVE-2016-4675**		
Apple Tv; Iphone Os; Watch Os Apple TV gives you access to everything you want to see and hear — like movies, music, photos, games, news and sports; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-4680**	https://support.apple.com/HT207271	O-APP-APPLE-030317/260
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-4665**	https://support.apple.com/HT207271	O-APP-APPLE-030317/261
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-4664**	https://support.apple.com/HT207271	O-APP-APPLE-030317/262
Denial of Service; Execute Code; Overflow;	20-02-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.2 is affected. tvOS before 10.1 is affected. watchOS	https://support.apple.com/HT207487	O-APP-APPLE-030317/263

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Memory Corruption			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. **CVE ID: CVE-2016-7626**		
Apple Tv;Mac Os X;Watch Os Apple TV gives you access to everything you want to see and hear — like movies, music, photos, games, news and sports; iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Denial of Service; Execute Code; Overflow	20-02-2017	6.8	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. **CVE ID: CVE-2016-4688**	https://support.apple.com/HT207269	O-APP-APPLE-030317/264
Iphone Os iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc.					
Bypass	20-02-2017	2.1	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. **CVE ID: CVE-2017-2351**	https://support.apple.com/HT207482	O-APP-IPHON-030317/265
Gain Information	20-02-2017	2.1	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue	https://support.apple.com/HT207	O-APP-IPHON-030317/266

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			involves the "Clipboard" component, which allows physically proximate attackers to obtain sensitive information in the lockscreen state by viewing clipboard contents. **CVE ID: CVE-2016-7765**	422	
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7759**	https://support.apple.com/HT207143	O-APP-IPHON-030317/267
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7664**	https://support.apple.com/HT207422	O-APP-IPHON-030317/268
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7653**	https://support.apple.com/HT207422	O-APP-IPHON-030317/269
Bypass	20-02-2017	2.1	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	https://support.apple.com/HT207422	O-APP-IPHON-030317/270

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			bypassing authentication. **CVE ID: CVE-2016-7638**		
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7634**	https://support.apple.com/HT207422	O-APP-IPHON-030317/271
NA	20-02-2017	2.1	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. **CVE ID: CVE-2016-7597**	https://support.apple.com/HT207422	O-APP-IPHON-030317/272
NA	20-02-2017	3.6	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. **CVE ID: CVE-2016-4686**	https://support.apple.com/HT207271	O-APP-IPHON-030317/273
NA	20-02-2017	4.3	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. **CVE ID: CVE-2017-2371**	https://support.apple.com/HT207482	O-APP-IPHON-030317/274
Denial of Service	20-02-2017	4.3	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. **CVE ID: CVE-2017-2368**	https://support.apple.com/HT207482	O-APP-IPHON-030317/275

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Cross Site Scripting	20-02-2017	4.3	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. **CVE ID: CVE-2016-7762**	https://support.apple.com/HT207422	O-APP-IPHON-030317/276
Denial of Service	20-02-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "Graphics Driver" component, which allows remote attackers to cause a denial of service via a crafted video. **CVE ID: CVE-2016-7665**	https://support.apple.com/HT207422	O-APP-IPHON-030317/277
Denial of Service	20-02-2017	4.3	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. **CVE ID: CVE-2016-7581**	https://support.apple.com/HT207271	O-APP-IPHON-030317/278
NA	20-02-2017	4.3	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. **CVE ID: CVE-2016-4685**	https://support.apple.com/HT207271	O-APP-IPHON-030317/279
NA	20-02-2017	4.6	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. **CVE ID: CVE-2016-7601**	https://support.apple.com/HT207422	O-APP-IPHON-030317/280
Bypass	20-02-2017	4.6	An issue was discovered in certain Apple products. iOS before 10.2 is affected. The issue involves the "SpringBoard"	https://support.apple.com/HT207422	O-APP-IPHON-030317/281

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			component, which allows physically proximate attackers to bypass the passcode attempt counter and unlock a device via unspecified vectors. **CVE ID: CVE-2016-4781**		
Execute Code	20-02-2017	4.6	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. **CVE ID: CVE-2016-4690**	https://support.apple.com/HT207422	O-APP-IPHON-030317/282
NA	20-02-2017	5	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. **CVE ID: CVE-2016-4689**	https://support.apple.com/HT207422	O-APP-IPHON-030317/283
Bypass	20-02-2017	7.5	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 mechanism via unspecified vectors. **CVE ID: CVE-2016-7630**	https://support.apple.com/HT207422	O-APP-IPHON-030317/284
Iphone Os;Mac Os X iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc; macOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers ("Macs"), having been preinstalled on all Macs since 2002.					
NA	20-02-2017	2.1	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. **CVE ID: CVE-2016-4670**	https://support.apple.com/HT207275	O-APP-IPHON-030317/285

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Memory Corruption; Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7577**	https://support.apple.com/HT207275	O-APP-IPHON-030317/286
NA	20-02-2017	4.3	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. **CVE ID: CVE-2016-4721**	https://support.apple.com/HT207275	O-APP-IPHON-030317/287
Denial of Service	20-02-2017	5	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. **CVE ID: CVE-2016-7667**	https://support.apple.com/HT207423	O-APP-IPHON-030317/288
Denial of Service; Gain Privileges	20-02-2017	6.8	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. **CVE ID: CVE-2016-7655**	https://support.apple.com/HT207423	O-APP-IPHON-030317/289
Gain Privileges	20-02-2017	7.2	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	https://support.apple.com/HT207422	O-APP-IPHON-030317/290

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Management" component. It allows local users to gain privileges via unspecified vectors related to Mach port name references. **CVE ID: CVE-2016-7661**		
Iphone Os;Mac Os X;Watch Os iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc; MacOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers ("Macs"), having been preinstalled on all Macs since 2002; WatchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7714**	https://support.apple.com/HT207487	O-APP-IPHON-030317/291
NA	20-02-2017	2.1	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 related to symlinks. **CVE ID: CVE-2016-7619**	https://support.apple.com/HT207487	O-APP-IPHON-030317/292
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2016-7657**	https://support.apple.com/HT207487	O-APP-IPHON-030317/293
Denial of Service	20-02-2017	4.3	An issue was discovered in certain Apple products. iOS	https://support.apple.c	O-APP-IPHON-

			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. **CVE ID: CVE-2016-7636**	om/HT207487	030317/294
Denial of Service	20-02-2017	4.3	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. **CVE ID: CVE-2016-7627**	https://support.apple.com/HT207487	O-APP-IPHON-030317/295
Gain Information	20-02-2017	4.3	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 attackers to obtain sensitive information from kernel memory via a crafted app. **CVE ID: CVE-2016-7607**	https://support.apple.com/HT207487	O-APP-IPHON-030317/296
Denial of Service	20-02-2017	4.9	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. **CVE ID: CVE-2016-7615**	https://support.apple.com/HT207487	O-APP-IPHON-030317/297
NA	20-02-2017	5	An issue was discovered in certain Apple products. iOS before 10.2 is affected. macOS	https://support.apple.com/HT207	O-APP-IPHON-030317/298

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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. **CVE ID: CVE-2016-7662**	422	
Bypass	20-02-2017	5	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 makes it easier for attackers to bypass cryptographic protection mechanisms by leveraging use of the 3DES cipher. **CVE ID: CVE-2016-4693**	https://support.apple.com/HT207487	O-APP-IPHON-030317/299
Denial of Service; Gain Information	20-02-2017	5.8	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 from process memory or cause a denial of service (out-of-bounds read and application crash) via a crafted web site. **CVE ID: CVE-2016-7643**	https://support.apple.com/HT207422	O-APP-IPHON-030317/300
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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.	https://support.apple.com/HT207422	O-APP-IPHON-030317/301

			CVE ID: CVE-2016-7659		
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7658**	https://support.apple.com/HT207487	O-APP-IPHON-030317/302
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7595**	https://support.apple.com/HT207487	O-APP-IPHON-030317/303
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-7594**	https://support.apple.com/HT207487	O-APP-IPHON-030317/304
Denial of Service; Execute Code; Overflow Memory	20-02-2017	6.8	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.	https://support.apple.com/HT207487	O-APP-IPHON-030317/305

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Corruption			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. **CVE ID: CVE-2016-7588**		
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-4691**	https://support.apple.com/HT207487	O-APP-IPHON-030317/306
Gain Privileges	20-02-2017	7.2	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. **CVE ID: CVE-2016-7660**	https://support.apple.com/HT207422	O-APP-IPHON-030317/307
Denial of Service; Overflow; Gain Privileges; Memory Corruption	20-02-2017	7.2	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. **CVE ID: CVE-2016-7637**	https://support.apple.com/HT207487	O-APP-IPHON-030317/308

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service; Execute Code	20-02-2017	7.2	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. **CVE ID: CVE-2016-7621**	https://support.apple.com/HT207487	O-APP-IPHON-030317/309
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	7.5	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. **CVE ID: CVE-2016-7663**	https://support.apple.com/HT207422	O-APP-IPHON-030317/310
Denial of Service; Execute Code	20-02-2017	9.3	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 (use-after-free) via a crafted app. **CVE ID: CVE-2016-7644**	https://support.apple.com/HT207487	O-APP-IPHON-030317/311
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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	https://support.apple.com/HT207487	O-APP-IPHON-030317/312

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2016-7616**		
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-7612**	https://support.apple.com/HT207487	O-APP-IPHON-030317/313
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-7606**	https://support.apple.com/HT207487	O-APP-IPHON-030317/314
Denial of Service; Execute Code	20-02-2017	9.3	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. **CVE ID: CVE-2016-7591**	https://support.apple.com/HT207487	O-APP-IPHON-030317/315
Iphone Os;Watch Os iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Bypass	20-02-2017	2.1	An issue was discovered in certain Apple products. iOS	https://support.apple.c	O-APP-IPHON-

			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. **CVE ID: CVE-2017-2352**	om/HT207 487	030317/316
Bypass	20-02-2017	4.6	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. **CVE ID: CVE-2016-7651**	https://support.apple.com/HT207 422	O-APP-IPHON-030317/317
Mac Os X MacOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc. designed to run on Apple's Macintosh computers ("Macs"), having been preinstalled on all Macs since 2002.					
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7761**	https://support.apple.com/HT207 423	O-APP-MAC O-030317/318
Bypass	20-02-2017	2.1	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. **CVE ID: CVE-2016-7628**	https://support.apple.com/HT207 423	O-APP-MAC O-030317/319
Gain Information	20-02-2017	2.1	An issue was discovered in certain Apple products. macOS	https://support.apple.c	O-APP-MAC O-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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. **CVE ID: CVE-2016-7625**	om/HT207 423	030317/320
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7624**	https://support.apple.com/HT207 423	O-APP-MACO-030317/321
Gain Information	20-02-2017	2.1	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. **CVE ID: CVE-2016-7620**	https://support.apple.com/HT207 423	O-APP-MACO-030317/322
Gain Information	20-02-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "IOFireWireFamily" component, which allows local users to obtain sensitive information from kernel memory via unspecified vectors. **CVE ID: CVE-2016-7608**	https://support.apple.com/HT207 423	O-APP-MACO-030317/323
Gain Information	20-02-2017	2.1	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.	https://support.apple.com/HT207 423	O-APP-MACO-030317/324

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CVE ID: CVE-2016-7600		
Cross Site Scripting	20-02-2017	4.3	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. **CVE ID: CVE-2017-2361**	https://support.apple.com/HT207483	O-APP-MACO-030317/325
Gain Information	20-02-2017	4.3	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. **CVE ID: CVE-2017-2357**	https://support.apple.com/HT207483	O-APP-MACO-030317/326
Denial of Service	20-02-2017	4.3	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. **CVE ID: CVE-2016-7605**	https://support.apple.com/HT207423	O-APP-MACO-030317/327
Denial of Service	20-02-2017	4.3	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. **CVE ID: CVE-2016-7580**	https://support.apple.com/HT207170	O-APP-MACO-030317/328
Denial of Service; Overflow; Memory Corruption	20-02-2017	4.3	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. **CVE ID: CVE-2016-4663**	https://support.apple.com/HT207275	O-APP-MACO-030317/329
Denial of	20-02-2017	4.3	An issue was discovered in	https://sup	O-APP-MAC

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Service			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. **CVE ID: CVE-2016-4661**	port.apple.com/HT207275	O-030317/330
Denial of Service; Gain Privileges	20-02-2017	4.6	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. **CVE ID: CVE-2016-4678**	https://support.apple.com/HT207275	O-APP-MAC O-030317/331
Denial of Service; Overflow; Gain Privileges; Memory Corruption	20-02-2017	4.6	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. **CVE ID: CVE-2016-4674**	https://support.apple.com/HT207275	O-APP-MAC O-030317/332
NA	20-02-2017	4.6	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. **CVE ID: CVE-2016-4617**	https://support.apple.com/HT207170	O-APP-MAC O-030317/333
Denial of Service	20-02-2017	4.9	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. **CVE ID: CVE-2016-7609**	https://support.apple.com/HT207423	O-APP-MAC O-030317/334

Denial of Service	20-02-2017	4.9	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. **CVE ID: CVE-2016-7604**	https://support.apple.com/HT207423	O-APP-MACO-030317/335
Denial of Service	20-02-2017	4.9	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. **CVE ID: CVE-2016-7603**	https://support.apple.com/HT207423	O-APP-MACO-030317/336
Denial of Service; Gain Information	20-02-2017	5.8	An issue was discovered in certain Apple products. macOS before 10.12 is affected. macOS before 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. **CVE ID: CVE-2016-4682**	https://support.apple.com/HT207275	O-APP-MACO-030317/337
Execute Code	20-02-2017	6.8	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. **CVE ID: CVE-2016-7742**	https://support.apple.com/HT207423	O-APP-MACO-030317/338
Denial of Service; Execute Code; Overflow; Memory Corruption	20-02-2017	6.8	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	https://support.apple.com/HT207423	O-APP-MACO-030317/339

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			code or cause a denial of service (memory corruption and application crash) via a crafted .gcx file. **CVE ID: CVE-2016-7622**		
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves 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. **CVE ID: CVE-2016-7618**	https://support.apple.com/HT207423	O-APP-MACO-030317/340
Denial of Service; Execute Code; Overflow	20-02-2017	6.8	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. **CVE ID: CVE-2016-4683**	https://support.apple.com/HT207275	O-APP-MACO-030317/341
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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. **CVE ID: CVE-2016-4681**	https://support.apple.com/HT207275	O-APP-MACO-030317/342
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	6.8	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 (memory corruption and	https://support.apple.com/HT207275	O-APP-MACO-030317/343

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			application crash) via a crafted font. **CVE ID: CVE-2016-4667**		
Denial of Service; Gain Privileges	20-02-2017	7.2	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. **CVE ID: CVE-2016-7633**	https://support.apple.com/HT207423	O-APP-MACO-030317/344
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2017-2358**	https://support.apple.com/HT207483	O-APP-MACO-030317/345
Denial of Service; Execute Code	20-02-2017	9.3	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. **CVE ID: CVE-2017-2353**	https://support.apple.com/HT207483	O-APP-MACO-030317/346
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.2 is affected. The issue involves the "kext tools" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2016-7629**	https://support.apple.com/HT207423	O-APP-MACO-030317/347
Denial of Service;	20-02-2017	9.3	An issue was discovered in certain Apple products. macOS	https://support.apple.c	O- APP-MACO-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Execute Code			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. **CVE ID: CVE-2016-7617**	om/HT207423	030317/348
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-7602**	https://support.apple.com/HT207423	O-APP-MACO-030317/349
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-7596**	https://support.apple.com/HT207423	O-APP-MACO-030317/350
Denial of Service; Execute Code; Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-7582**	https://support.apple.com/HT207170	O-APP-MACO-030317/351
Denial of Service; Execute Code	20-02-2017	9.3	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	https://support.apple.com/HT207275	O-APP-MACO-030317/352

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **CVE ID: CVE-2016-4780**		
Denial of Service; Execute Code	20-02-2017	9.3	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. **CVE ID: CVE-2016-4671**	https://support.apple.com/HT207275	O-APP-MACO-030317/353
Denial of Service; Execute Code; Overflow Memory Corruption	20-02-2017	9.3	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. **CVE ID: CVE-2016-4662**	https://support.apple.com/HT207275	O-APP-MACO-030317/354
Cisco					
Email Security Appliance Firmware;Web Security Appliance A security appliance is any form of server appliance that is designed to protect computer networks from unwanted traffic.					
Bypass	21-02-2017	5	Vulnerability in the Multipurpose Internet Mail Extensions (MIME) scanner of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) and Web Security Appliances (WSA) could allow an unauthenticated, remote attacker to bypass configured user filters on the device. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco ESA and Cisco WSA, both	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-asyncos	O-CIS-EMAIL-030317/355

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			virtual and hardware appliances, that are configured with message or content filters to scan incoming email attachments on the ESA or services scanning content of web access on the WSA. More Information: SCvb91473, CSCvc76500. Known Affected Releases: 10.0.0-203 9.9.9-894 WSA10.0.0-233. **CVE ID: CVE-2017-3827**		
Dell					
Sonicwall Secure Remote Access Server Designed for organizations with up to 250 remote employees, the SonicWall Secure Remote Access (SRA) 4600 Appliance provides medium-sized businesses with a high performing, easy-to-use and cost-effective SRA solutions that require no pre-installed client software.					
NA	22-02-2017	10	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. **CVE ID: CVE-2016-9684**	http://documents.software.dell.com/sonicwall-sma-100-series/8.1.0.7/release-notes/resolved-issues?ParentProduct=868	O-DEL-SONIC-030317/356
NA	22-02-2017	10	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)	http://documents.software.dell.com/sonicwall-sma-100-series/8.1.0.7/release-	O-DEL-SONIC-030317/357

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			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. **CVE ID: CVE-2016-9683**	notes/resolved-issues?ParentProduct=868	
NA	22-02-2017	10	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. **CVE ID: CVE-2016-9682**	http://documents.software.dell.com/sonicwall-sma-100-series/8.1.0.7/release-notes/resolved-issues?ParentProduct=868	O-DEL-SONIC-030317/358
Digisol					
Dg-hr1400 Firmware NA					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Cross Site Request Forgery	21-02-2017	6.8	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. **CVE ID: CVE-2017-6127**	NA	O-DIG-DG-HR-030317/359
Dlink					
Websmart Dgs-1510 Series Firmware The DGS-1510 Series is D-Link's latest generation of SmartPro switches with 10G port connectivity, making them ideal for deployment in SME/SMB aggregation environments.					
Gain Information	23-02-2017	5	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. **CVE ID: CVE-2017-6206**	http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10070	O-DLI-WEBSM-030317/360
Bypass	23-02-2017	7.5	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. **CVE ID: CVE-2017-6205**	http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10070	O-DLI-WEBSM-030317/361
Linux					
Linux Kernel The Linux kernel is a monolithic Unix-like computer operating system kernel.					
Bypass	24-02-2017	4.6	The do_shmat function in ipc/shm.c in the Linux kernel	https://github.com/to	O-LIN-LINUX-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			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. **CVE ID: CVE-2017-5669**	rvalds/linux/commit/e1d35d4dc7f089e6c9c080d556feedf9c706f0c7	030317/362
Denial of Service	23-02-2017	5	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. **CVE ID: CVE-2017-6214**	https://github.com/torvalds/linux/commit/ccf7abb93af09ad0868ae9033d1ca8108bdaec82	O-LIN-LINUX-030317/363
Denial of Service	18-02-2017	7.1	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. **CVE ID: CVE-2017-5986**	https://github.com/torvalds/linux/commit/2dcab598484185dea7ec22219c76dcdd59e3cb90	O-LIN-LINUX-030317/364
Denial of Service; Overflow; Memory Corruption; Gain Information	22-02-2017	7.2	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. **CVE ID: CVE-2016-8636**	https://bugzilla.redhat.com/show_bug.cgi?id=1421981	O-LIN-LINUX-030317/365

Gain Privileges	18-02-2017	7.6	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 context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786. **CVE ID: CVE-2017-6001**	https://github.com/torvalds/linux/commit/321027c1fe77f892f4ea07846aeae08cefbbb290	O-LIN-LINUX-030317/366
Denial of Service	18-02-2017	9.3	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. **CVE ID: CVE-2017-6074**	https://github.com/torvalds/linux/commit/5edabca9d4cff7f1f2b68f0bac55ef99d9798ba4	O-LIN-LINUX-030317/367
Netgear					
Dgn2200 Firmware NA					
Execute Code	22-02-2017	10	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. **CVE ID: CVE-2017-6077**	NA	O-NET-DGN22-030317/368
XEN					
XEN Xen Project is a hypervisor using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.					
Gain Information	22-02-2017	2.1	Xen 4.7 allows local guest OS users to obtain sensitive host	http://xenbits.xen.org	O-XEN-XEN-030317/369

			information by loading a 32-bit ELF symbol table. **CVE ID: CVE-2016-9384**	/xsa/xsa194.patch	
Denial of Service	22-02-2017	2.1	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 an incorrect choice for software interrupt delivery. **CVE ID: CVE-2016-9378**	http://xenbits.xen.org/xsa/advisory-196.html	O-XEN-XEN-030317/370
Denial of Service	22-02-2017	2.1	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. **CVE ID: CVE-2016-9377**	http://xenbits.xen.org/xsa/advisory-196.html	O-XEN-XEN-030317/371
Denial of Service	27-02-2017	4.9	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving an asynchronous abort while at HYP. **CVE ID: CVE-2016-9818**	http://xenbits.xen.org/xsa/advisory-201.html	O-XEN-XEN-030317/372
Denial of Service	27-02-2017	4.9	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving a (1) data or (2) prefetch abort with the ESR_EL2.EA bit set. **CVE ID: CVE-2016-9817**	http://xenbits.xen.org/xsa/advisory-201.html	O-XEN-XEN-030317/373
Denial of Service	27-02-2017	4.9	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving an asynchronous abort while at EL2. **CVE ID: CVE-2016-9816**	http://xenbits.xen.org/xsa/advisory-201.html	O-XEN-XEN-030317/374

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service	27-02-2017	4.9	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host panic) by sending an asynchronous abort. **CVE ID: CVE-2016-9815**	http://xenbits.xen.org/xsa/xsa201-1.patch	O-XEN-XEN-030317/375
Zyxel					
Nwa3560-n Firmware;Usg50 Firmware NA					
Denial of Service	21-02-2017	7.8	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. **CVE ID: CVE-2016-10227**	NA	O-ZYX-NWA35-030317/376

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**