GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Monday, January 14, 2019
GLESEC-CSFR0043

SB19-014: Vulnerability Summary for the Week of January 7, 2019

Original release date: January 14, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.	2019-01-08	7.6	CVE-2019-0565 BID CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arc_project -- arc	ARC 5.21q allows directory traversal via a full pathname in an archive file.	2019-01-07	5.0	CVE-2015-9275 MISC MISC
getbootstrap -- bootstrap	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	2019-01-09	4.3	CVE-2016-10735 MISC MISC MISC MISC MISC MISC
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.4 could allow a user authenticated as an administrator with limited rights to escalate their privileges. IBM X-Force ID: 151258.	2019-01-04	6.5	CVE-2018-1859 BID XF CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- asp.net_core	A denial of service vulnerability exists when ASP.NETCore improperly handles web requests, aka "ASP.NETCore Denial of Service Vulnerability." This affects ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0548.	2019-01-08	5.0	CVE-2019-0564 BID REDHAT CONFIRM
microsoft -- office	An information disclosure vulnerability exists when Microsoft Outlook improperly handles certain types of messages, aka "Microsoft Outlook Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2019-01-08	4.3	CVE-2019-0559 BID CONFIRM
microsoft -- office	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka "Microsoft Office Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office.	2019-01-08	4.3	CVE-2019-0560 BID CONFIRM
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	4.3	CVE-2019-5310 MISC
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index cw parameter.	2019-01-04	4.3	CVE-2019-5311 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frog_cms_project -- frog_cms	Frog CMS 0.9.5 has XSS in the admin/?/page/edit/1 body field.	2019-01-09	3.5	CVE-2018-20680 MISC
ibm -- rational_publishing_engine	IBM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 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 X-force ID: 144883.	2019-01-04	3.5	CVE-2018-1657 BID XF CONFIRM
ibm -- rational_publishing_engine	IBM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 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 X-Force ID: 153494.	2019-01-04	3.5	CVE-2018-1951 BID XF CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- karaf	Apache Karaf provides a features deployer, which allows users to "hot deploy" a features XML by dropping the file directly in the deploy folder. The features XML is parsed by XMLInputFactory class. Apache Karaf XMLInputFactory class doesn't contain any mitigation codes against XXE. This is a potential security risk as an user can inject external XML entities in Apache Karaf version prior to 4.1.7 or 4.2.2. It has been fixed in Apache Karaf 4.1.7 and 4.2.2 releases.	2019-01-07	not yet calculated	CVE-2018-11788 MISC BID
apache -- thrift	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	2019-01-07	not yet calculated	CVE-2018-1320 MISC
apache -- thrift	The Apache Thrift Node.js static web server in versions 0.9.2	2019-01-07	not yet	CVE-2018-

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.		calculated	11798 BID MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the Clean My Mac X, version 4.04, helper service due to improper input validation. A user with local access can use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	CVE-2018-4043 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4047 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the way the CleanMyMac X software improperly validates inputs. An attacker with local	2019-01-10	not yet calculated	CVE-2018-4032 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access could use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.			
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4033 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4034 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4045 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege	2019-01-10	not yet	CVE-2018-

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the running kernel extensions on the system.		calculated	4036 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access can use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4037 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4035 MISC
apple -- cleanmymac_x	An exploitable denial-of-service vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. A user with local access can use this vulnerability to terminate a privileged helper application. An attacker would	2019-01-10	not yet calculated	CVE-2018-4046 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	need local access to the machine for a successful exploit.			
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4041 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4042 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4044 MISC
apple -- ios	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was	2019-01-11	not yet	CVE-2017-2411

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	addressed by enabling HTTPS for exchange rates.		calculated	CONFIRM
apple -- ios	In iOS before 11.4 and macOS High Sierra before 10.13.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4404 MISC CONFIRM EXPLOIT-DB
apple -- ios	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	not yet calculated	CVE-2017-13891 CONFIRM
apple -- ios	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2017-13888 CONFIRM
apple -- ios	In iOS before 11.4, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4330 BID SECTRACK CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ios	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	not yet calculated	CVE-2016-7576 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	CVE-2018-4257 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4255 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4254 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	not yet calculated	CVE-2018-4217 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	not yet calculated	CVE-2018-4183 CONFI

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	not yet calculated	CVE-2018-4182 CONFIRM DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	CVE-2018-4181 MLIST CONFIRM UBUNTU DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	CVE-2018-4180 MLIST CONFIRM UBUNTU

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	not yet calculated	CVE-2018-4258 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4256 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.4, there was an issue with the handling of smartcard PINs. This issue was addressed with additional logic.	2019-01-11	not yet calculated	CVE-2018-4179 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, an access issue existed with privileged WiFi system configuration. This issue was addressed with additional restrictions.	2019-01-11	not yet calculated	CVE-2017-13886 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, a logic issue existed in APFS when deleting keys during hibernation. This was addressed with improved state management.	2019-01-11	not yet calculated	CVE-2017-13887 CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4194 MISC CONFIRM MISC MISC MISC
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	not yet calculated	CVE-2017-13889 CONFIRM
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4169 CONFIRM
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be	2019-01-11	not yet calculated	CVE-2018-4278 SECTRACK GENT

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.			OO CONFIRM MISC MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4277 SECTRACK MISC MISC MISC CONFIRM MISC
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4262 SECTRACK GENTOO MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4213 GENTOO MISC CONFIRM MISC MISC MISC UBUNTU
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	not yet calculated	CVE-2018-4298 CONFIRM MISC
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected	2019-01-11	not yet calculated	CVE-2018-4212 GENTOO

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interaction causes an ASSERT failure. This issue was addressed with improved checks.			MISC CONFIRM MISC MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4210 GENTOO MISC MISC MISC CONFIRM UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4209 GENTOO MISC CONFIRM MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4208 GENTOO MISC MISC MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4207 GENTOO MISC CONFIRM MISC MISC MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC UBUNTU
apple -- multiple_products	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4189 CONFIRM MISC MISC MISC
apple -- multiple_products	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4147 CONFIRM MISC MISC MISC MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the	2019-01-11	not yet calculated	CVE-2016-4644 MISC MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication types with the credentials.			
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	not yet calculated	CVE-2016-4643 MISC MISC CONFIRM
apple -- multiple_products	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	CVE-2018-4185 MISC MISC CONFIRM MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	not yet calculated	CVE-2016-4642 MISC MISC CONFIRM
apple -- safari	In Safari before 11.1, an information leakage issue existed	2019-01-11	not yet	CVE-2018-

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in the handling of downloads in Safari Private Browsing. This issue was addressed with additional validation.		calculated	4186 CONFIRM
apple -- swiftnio	In SwiftNIO before 1.8.0, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	CVE-2018-4281 CONFIRM
artifex -- mupdf	Artifex MuPDF 1.14.0 has a SEGV in the function fz_load_page of the fitz/document.c file, as demonstrated by mutool. This is related to page-number mishandling in cbz/mucbz.c, cbz/muimg.c, and svg/svg-doc.c.	2019-01-11	not yet calculated	CVE-2019-6130 MISC
artifex -- mupdf	svg-run.c in Artifex MuPDF 1.14.0 has infinite recursion with stack consumption in svg_run_use_symbol, svg_run_element, and svg_run_use, as demonstrated by mutool.	2019-01-11	not yet calculated	CVE-2019-6131 MISC
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter or	2019-01-09	not yet calculated	CVE-2018-0634 MISC JVN

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bootmode parameter of a certain URL.			
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via filename parameter.	2019-01-09	not yet calculated	CVE-2018-0635 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter of a certain URL, different URL from CVE-2018-0634.	2019-01-09	not yet calculated	CVE-2018-0636 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via import.cgi encKey parameter.	2019-01-09	not yet calculated	CVE-2018-0638 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via tools_firmware.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	CVE-2018-0639 MISC JVN
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator	2019-01-09	not yet	CVE-2018-0640

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	rights to execute arbitrary code via netWizard.cgi date parameter, time parameter, and offset parameter.		calculated	MISC JVN
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via tools_system.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	CVE-2018-0641 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via export.cgi encKey parameter.	2019-01-09	not yet calculated	CVE-2018-0637 MISC JVN
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via submit-url parameter.	2019-01-09	not yet calculated	CVE-2018-0633 MISC JVN
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0632 MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute	2019-01-09	not yet	CVE-2018-0631

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary OS commands via targetAPSsid parameter.		calculated	MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0629 MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd parameter.	2019-01-09	not yet calculated	CVE-2018-0630 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0628 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSsid parameter.	2019-01-09	not yet calculated	CVE-2018-0627 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS	2019-01-09	not yet calculated	CVE-2018-0626 MISC JVN

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	commands via sysCmd in formWsc parameter.			
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via formSysCmd parameter.	2019-01-09	not yet calculated	CVE-2018-0625 MISC JVN
bento4 -- bento4	An issue was discovered in Bento4 v1.5.1-627. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/Ap4DescriptorFactory.cpp when called from the AP4_EsdsAtom class in Core/Ap4EsdsAtom.cpp, as demonstrated by mp42aac.	2019-01-11	not yet calculated	CVE-2019-6132 MISC
bodhi -- bodhi	Bodhi 2.9.0 and lower is vulnerable to cross-site scripting resulting in code injection caused by incorrect validation of bug titles.	2019-01-10	not yet calculated	CVE-2017-1002152 CONFIRM
bootstrap -- bootstrap	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	2019-01-09	not yet calculated	CVE-2018-20677 MISC MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC
bootstrap -- bootstrap	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	2019-01-09	not yet calculated	CVE-2018-20676 MISC MISC MISC MISC MISC
busybox -- busybox	An issue was discovered in BusyBox through 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and/or relay) might allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to assurance of a 4-byte length when decoding DHCP_SUBNET. NOTE: this issue exists because of an incomplete fix for CVE-2018-20679.	2019-01-09	not yet calculated	CVE-2019-5747 MISC MISC
busybox -- busybox	An issue was discovered in BusyBox before 1.30.0. An out of bounds read in udhcp	2019-01-09	not yet	CVE-2018-20679

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes.		calculated	MISC MISC MISC
cimtechniques -- cimscan	In CIMTechniques CIMScan 6.x through 6.2, the SOAP WSDL parser allows attackers to execute SQL code.	2019-01-10	not yet calculated	CVE-2018-16803 MISC MISC
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact	2019-01-11	not yet calculated	CVE-2018-15464 CISCO

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	services running on the device, resulting in a partial DoS condition.			
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the Secure/Multipurpose Internet Mail Extensions (S/MIME) Decryption and Verification or S/MIME Public Key Harvesting features of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause an affected device to corrupt system memory. A successful exploit could cause the filtering process to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. The vulnerability is due to improper input validation of S/MIME-signed emails. An attacker could exploit this vulnerability by sending a malicious S/MIME-signed email through a targeted device. If Decryption and Verification or Public Key Harvesting is configured, the filtering process could crash due to memory corruption and restart,	2019-01-10	not yet calculated	CVE-2018-15453 BID CISCO

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	resulting in a DoS condition. The software could then resume processing the same S/MIME-signed email, causing the filtering process to crash and restart again. A successful exploit could allow the attacker to cause a permanent DoS condition. This vulnerability may require manual intervention to recover the ESA.			
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device. The vulnerability is due to improper filtering of email messages that contain references to whitelisted URLs. An attacker could exploit this vulnerability by sending a malicious email message that contains a large number of whitelisted URLs. A successful exploit could allow the attacker to cause a sustained DoS condition	2019-01-10	not yet calculated	CVE-2018-15460 BID CISCO

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that could force the affected device to stop scanning and forwarding email messages.			

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY FLASH REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).

Credits:

Homeland Security

US-CERT United States Computer Emergency Readiness Team