GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Tuesday, January 8, 2019
GLESEC-CSFR0042

National Cyber Awareness System:

SB19-007: Vulnerability Summary for the Week of December 31, 2018

01/07/2019 06:55 AM EST

Original release date: January 07, 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

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

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.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
There were no high vulnerabilities recorded this week.				

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. It allows full path disclosure in "Smarty error: unable to read resource" error messages for a crafted installation page.	2018-12-28	5.0	CVE-2018-20566 MISC
f5 -- big-ip_access_policy_manager	A cross-site request forgery (CSRF) vulnerability in the APM webtop 11.2.1 or greater may allow attacker to force an APM webtop session to	2018-12-28	4.3	CVE-2018-15334 BID CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	log out and require re-authentication.			
freedesktop -- poppler	A reachable Object::getString assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to construction of invalid rich media annotation assets in the AnnotRichMedia class in Annot.c.	2018-12-28	4.3	CVE-2018-20551 MISC MISC
freedesktop -- poppler	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a check for the dict data type, as demonstrated by use of the FileSpec class (in FileSpec.cc) in pdfdetach.	2019-01-01	4.3	CVE-2018-20650 MISC MISC
libming -- libming	A heap-based buffer over-read was discovered in decompileJUMP function in util/decompile.c of libming v0.4.8. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by swftocxx.	2018-12-30	4.3	CVE-2018-20591 MISC
tinyexr_project -- tinyexr	An attempted excessive memory allocation was discovered in the function tinyexr::AllocateImage in tinyexr.h in tinyexr v0.9.5. Remote attackers could leverage this vulnerability to cause a denial-of-service via crafted input, which leads to an out-of-memory exception.	2019-01-01	4.3	CVE-2018-20652 MISC
ucms_project -- ucms	UCMS 1.4.7 has ?do=user_addpost CSRF.	2018-12-30	6.8	CVE-2018-

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

				20598 MISC
ucms_project -- ucms	UCMS 1.4.7 allows remote attackers to execute arbitrary PHP code by entering this code during an index.php sadmin_fileedit action.	2018-12-30	6.5	CVE-2018-20599 MISC
ucms_project -- ucms	sadmin\cedit.php in UCMS 1.4.7 has XSS via an index.php sadmin_cedit action.	2018-12-30	4.3	CVE-2018-20600 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/page.php?rec=edit has XSS via the page_name parameter.	2018-12-28	3.5	CVE-2018-20557 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/system.php?rec=update has XSS via the site_name parameter.	2018-12-28	3.5	CVE-2018-20558 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product.php?rec=update has XSS via the name parameter.	2018-12-28	3.5	CVE-2018-20559 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221.	2018-12-28	3.5	CVE-2018-

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	admin/show.php?rec=update has XSS via the show_name parameter.			20560 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article.php?rec=update has XSS via the title parameter.	2018-12-28	3.5	CVE-2018-20561 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	3.5	CVE-2018-20562 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/mobile.php?rec=system&act=update has XSS via the mobile_name parameter.	2018-12-28	3.5	CVE-2018-20563 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	3.5	CVE-2018-20564 MISC
douco -- douphp	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/nav.php?rec=update has XSS via the nav_name parameter.	2018-12-28	3.5	CVE-2018-20565 MISC
ucms_project -- ucms	UCMS 1.4.7 has XSS via the dir parameter in an index.php sadmin_fileedit action.	2018-12-30	3.5	CVE-2018-20597 MISC
ucms_project -- ucms	UCMS 1.4.7 has XSS via the description parameter in an index.php list_editpost action.	2018-12-30	3.5	CVE-2018-20601 MISC

website_seller_script_project -- website_seller_script	PHP Scripts Mall Website Seller Script 2.0.5 has XSS via a Profile field such as Company Address, a related issue to CVE-2018-15896.	2018-12-28	3.5	CVE-2018-20530 MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices ABB GATE-E1 and GATE-E2 all versions do not allow authentication to be configured on administrative telnet or web interfaces, which could enable various effects vectors, including conducting device resets, reading or modifying registers, and changing configuration settings such as IP addresses.	2019-01-03	not yet calculated	CVE-2018-18995 BID MISC
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices in ABB GATE-E1 and GATE-E2 all versions allows an unauthenticated attacker using the administrative web interface to insert an HTML/Javascript payload into any of the device properties, which may allow an attacker to display/execute the payload in a visitor browser.	2019-01-03	not yet calculated	CVE-2018-18997 BID MISC
ansible -- ansible	ansible before versions 2.5.14, 2.6.11, 2.7.5 is vulnerable to a information disclosure flaw in vvv+ mode with no_log	2019-01-03	not yet calculated	CVE-2018-16876 BID

	on that can lead to leakage of sensible data.			REDHAT REDHAT REDHAT REDHAT CONFIRM MISC
ansible -- tower	Ansible Tower before version 3.3.3 does not set a secure channel as it is using the default insecure configuration channel settings for messaging celery workers from RabbitMQ. This could lead in data leak of sensitive information such as passwords as well as denial of service attacks by deleting projects or inventory files.	2019-01-03	not yet calculated	CVE-2018-16879 BID CONFIRM
apache -- netbeans	Apache NetBeans (incubating) 9.0 NetBeans Proxy Auto-Configuration (PAC) interpretation is vulnerable for remote command execution (RCE). Using the nashorn script engine the environment of the javascript execution for the Proxy Auto-Configuration leaks privileged objects, that can be used to circumvent the execution limits. If a different script engine was used, no execution limits were in place. Both vectors allow remote code execution.	2018-12-31	not yet calculated	CVE-2018-17191 BID MISC
aria2 -- aria2	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which	2019-01-02	not yet calculated	CVE-2019-3500 MISC

	might allow local users to obtain sensitive information by reading this file.			
artifex -- ghostscript	In Artifex Ghostscript before 9.26, a carefully crafted PDF file can trigger an extremely long running computation when parsing the file.	2019-01-02	not yet calculated	CVE-2018-19478 CONFIRM BID CONFIRM CONFIRM MLIST CONFIRM
august -- connect_devices	An issue was discovered on August Connect devices. Insecure data transfer between the August app and August Connect during configuration allows attackers to discover home Wi-Fi credentials. This data transfer uses an unencrypted access point for these credentials, and passes them in an HTTP POST, using the AugustWifiDevice class, with data encrypted with a fixed key found obfuscated in the app.	2019-01-02	not yet calculated	CVE-2018-20100 MISC
bento4 -- bento4	An issue was discovered in Bento4 1.5.1-627. The AP4_StcoAtom class in Core/Ap4StcoAtom.cpp has an attempted excessive memory allocation when called from AP4_AtomFactory::CreateAtomFromStream in Core/Ap4AtomFactory.cpp, as demonstrated by mp42hls.	2019-01-02	not yet calculated	CVE-2018-20659 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

bmc -- remedy	Remedy AR System Server in BMC Remedy 7.1 may fail to set the correct user context in certain impersonation scenarios, which can allow a user to act with the identity of a different user, because userdata.js in the WOI:WorkOrderConsole component allows a username substitution involving a UserData_Init call.	2019-01-03	not yet calculated	CVE-2018-19505 MISC FULLDISC SECTRACK
buck -- buck	Buck parser-cache command loads/saves state using Java serialized object. If the state information is maliciously crafted, deserializing it could lead to code execution. This issue affects Buck versions prior to v2018.06.25.01.	2018-12-31	not yet calculated	CVE-2018-6331 MISC
chinamobile_plc -- wireless_router_gpn2.4p21-c-cn_devices	ChinaMobile PLC Wireless Router GPN2.4P21-C-CN devices with firmware W2001EN-00 have XSS via the cgi-bin/webproc?getpage=html/index.html var:subpage parameter.	2019-01-02	not yet calculated	CVE-2018-20326 MISC MISC MISC
cim -- cim	public\install\install.php in CIM 0.9.3 allows remote attackers to reload the product via the public/install/#/step3 URI.	2018-12-30	not yet calculated	CVE-2018-20614 MISC
code42 -- code42_for_enterprise	The Code42 app before 6.8.4, as used in Code42 for Enterprise, on Linux installs with overly permissive permissions on the /usr/local/crashplan/log directory. This allows a user to manipulate symbolic links to escalate privileges, or show the contents of sensitive files that a regular user would not have access to.	2019-01-02	not yet calculated	CVE-2018-20131 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

core_ftp_server -- core_ftp_server	The server in Core FTP 2.0 build 653 on 32-bit platforms allows remote attackers to cause a denial of service (daemon crash) via a crafted XRMD command.	2019-01-02	not yet calculated	CVE-2018-20658 MISC EXPLOIT-DB
couchdb -- couchdb	Prior to CouchDB version 2.3.0, CouchDB allowed for runtime-configuration of key components of the database. In some cases, this lead to vulnerabilities where CouchDB admin users could access the underlying operating system as the CouchDB user. Together with other vulnerabilities, it allowed full system entry for unauthenticated users. Rather than waiting for new vulnerabilities to be discovered, and fixing them as they come up, the CouchDB development team decided to make changes to avoid this entire class of vulnerabilities.	2019-01-02	not yet calculated	CVE-2018-17188 MISC
cuba_platform -- cuba_platform	The Reporting Addon (aka Reports Addon) through 2019-01-02 for CUBA Platform through 6.10.x has Persistent XSS via the "Reports > Reports" name field.	2019-01-03	not yet calculated	CVE-2018-20663 MISC
cuppacms -- cuppacms	CuppaCMS has XSS via an SVG document uploaded to the administrator/#/component/table_manager/view/cu_views URI.	2018-12-31	not yet calculated	CVE-2018-19918 CONFIRM MISC
d-link -- dir-818lw_and_dir-860l	On D-Link DIR-818LW Rev.A 2.05.B03 and DIR-860L Rev.B 2.03.B03 devices, unauthenticated remote OS command	2019-01-02	not yet	CVE-2018-

	execution can occur in the soap.cgi service of the cgibin binary via an "&&" substring in the service parameter. NOTE: this issue exists because of an incomplete fix for CVE-2018-6530.		calculated	20114 MISC
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to adherents/type.php.	2019-01-03	not yet calculated	CVE-2018-19992 MISC
dolibarr -- dolibarr	A reflected cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote attackers to inject arbitrary web script or HTML via the transphrase parameter to public/notice.php.	2019-01-03	not yet calculated	CVE-2018-19993 MISC
dolibarr -- dolibarr	An error-based SQL injection vulnerability in product/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the desiredstock parameter.	2019-01-03	not yet calculated	CVE-2018-19994 MISC
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to user/card.php.	2019-01-03	not yet calculated	CVE-2018-19995 MISC MISC
dolibarr -- dolibarr	SQL injection vulnerability in user/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the employee parameter.	2019-01-03	not yet calculated	CVE-2018-19998 MISC MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

driveragent -- driveragent	DriverAgent 2.2015.7.14, which includes DrvAgent64.sys 1.0.0.1, allows a user to send an IOCTL (0x80002068) with a user defined buffer size. If the size of the buffer is less than 512 bytes, then the driver will overwrite the next pool header if there is one next to the user buffer's pool.	2019-01-03	not yet calculated	CVE-2018-19523 MISC
emc -- rsa_archer	RSA Archer versions prior to 6.5.0.1 contain an improper access control vulnerability. A remote malicious user could potentially exploit this vulnerability to bypass authorization checks and gain read access to restricted user information.	2019-01-03	not yet calculated	CVE-2018-15780 BID FULLDISC
epon -- cpe-wifi_devices	EPON CPE-WiFi devices 2.0.4-X000 are vulnerable to escalation of privileges by sending cooLogin=1, cooUser=admin, and timestamp=-1 cookies.	2019-01-03	not yet calculated	CVE-2018-20512 MISC
exiftool -- exiftool	ExifTool 8.32 allows local users to gain privileges by creating a %TEMP%\par-%username%\cache-exiftool-8.32 folder with a victim's username, and then copying a Trojan horse ws32_32.dll file into this new folder, aka DLL Hijacking. NOTE: 8.32 is an obsolete version from 2010 (9.x was released starting in 2012, and 10.x was released starting in 2015).	2019-01-02	not yet calculated	CVE-2018-20211 MISC FULLDISC
expressvpn -- expressvpn	An issue was discovered in ExpressVPN on Windows. The Xvpnd.exe process (which runs as a service with SYSTEM privileges) listens on TCP port 2015, which is used as an RPC interface for communication with the client side of the ExpressVPN application. A JSON-RPC	2019-01-02	not yet calculated	CVE-2018-15490 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	protocol over HTTP is used for communication. The JSON-RPC XVPN.GetPreference and XVPN.SetPreference methods are vulnerable to path traversal, and allow reading and writing files on the file system on behalf of the service.			
f5 -- big-ip	When APM 13.0.0-13.1.x is deployed as an OAuth Resource Server, APM becomes a client application to an external OAuth authorization server. In certain cases when communication between the BIG-IP APM and the OAuth authorization server is lost, APM may not display the intended message in the failure response	2018-12-28	not yet calculated	CVE-2018-15335 BID CONFIRM
f5 -- big-ip	On versions 11.2.1. and greater, unrestricted Snapshot File Access allows BIG-IP system's user with any role, including Guest Role, to have access and download previously generated and available snapshot files on the BIG-IP configuration utility such as QKView and TCPDumps.	2018-12-28	not yet calculated	CVE-2018-15333 BID CONFIRM
f5 -- ip_infusion_zebos_and_ocnos	The BGP daemon (bgpd) in all IP Infusion ZebOS versions to 7.10.6 and all OcNOS versions to 1.3.3.145 allow remote attackers to cause a denial of service attack via an autonomous system (AS) path containing 8 or more autonomous system number (ASN) elements.	2018-12-28	not yet calculated	CVE-2018-17539 BID CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure	2019-01-02	not yet	CVE-2018-14718

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	to block the slf4j-ext class from polymorphic deserialization.		calculated	CONFIRM CONFIRM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the axis2-transport-jms class from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-19360 CONFIRM CONFIRM CONFIRM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the openjpa class from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-19361 CONFIRM CONFIRM CONFIRM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow attackers to conduct external XML entity (XXE) attacks by leveraging failure to block unspecified JDK classes from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-14720 CONFIRM CONFI

				RM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-14721 CONFIRM CONFIRM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the blaze-ds-opt and blaze-ds-core classes from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-14719 CONFIRM CONFIRM CONFIRM
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.	2019-01-02	not yet calculated	CVE-2018-19362 CONFIRM CONFIRM CONFIRM CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is an Out-of-Bounds Read Information Disclosure and crash due to a NULL pointer dereference when reading TIFF data during TIFF parsing.	2019-01-03	not yet calculated	CVE-2019-5007 CONFIRM
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is a NULL pointer dereference during PDF parsing.	2019-01-03	not yet calculated	CVE-2019-5006 CONFIRM
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. They allowed Denial of Service (application crash) via image data, because two bytes are written to the end of the allocated memory without judging whether this will cause corruption.	2019-01-03	not yet calculated	CVE-2019-5005 CONFIRM
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r348229), 11.2-RELEASE-p7, 12.0-STABLE(r342228), and 12.0-RELEASE-p1, insufficient validation of network-provided data in bootpd may make it possible for a malicious attacker to craft a bootp packet which could cause a stack buffer overflow. It is possible that the buffer overflow could lead to a Denial of Service or remote code execution.	2019-01-03	not yet calculated	CVE-2018-17161 BID FREEBSD
frog -- frog_cms	FROG CMS 0.9.5 has XSS via the admin/?/snippet/add name parameter, which is mishandled during an edit action, a related issue to CVE-2018-10319.	2018-12-31	not yet calculated	CVE-2018-19844 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

getsimple -- getsimple_cms	There is Stored XSS in GetSimple CMS 3.3.12 via the admin/edit.php "post-menu" parameter, a related issue to CVE-2018-16325.	2018-12-31	not yet calculated	CVE-2018-19845 MISC
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	CVE-2018-20673 MISC
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	CVE-2018-20671 MISC MISC
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, has a memory leak via a crafted string, leading to a denial of service (memory consumption), as demonstrated by cxxfilt, a related issue to CVE-2018-12698.	2019-01-02	not yet calculated	CVE-2018-20657 BID MISC
gnu -- binutils	In GNU Binutils 2.31.1, there is a use-after-free in the error function in elfcomm.c when called from the process_archive function in readelf.c via a crafted ELF file.	2018-12-31	not yet calculated	CVE-2018-20623 BID MISC
gnu -- binutils	A NULL pointer dereference was discovered in elf_link_add_object_symbols in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils	2019-01-01	not yet calculated	CVE-2018-20651 BID

	2.31.1. This occurs for a crafted ET_DYN with no program headers. A specially crafted ELF file allows remote attackers to cause a denial of service, as demonstrated by ld.			MISC MISC
guardzilla -- gz180_devices	The remote upgrade feature in Guardzilla GZ180 devices allow command injection via a crafted new firmware version parameter.	2018-12-31	not yet calculated	CVE-2018-18600
hhvm -- hhvm	The Memcache::getextendedstats function can be used to trigger an out-of-bounds read. Exploiting this issue requires control over memcached server hostnames and/or ports. This affects all supported versions of HHVM (3.30 and 3.27.4 and below).	2018-12-31	not yet calculated	CVE-2018-6340 MISC MISC
hhvm -- hhvm	A Malformed h2 frame can cause 'std::out_of_range' exception when parsing priority meta data. This behavior can lead to denial-of-service. This affects all supported versions of HHVM (3.25.2, 3.24.6, and 3.21.10 and below) when using the proxygen server to handle HTTP2 requests.	2018-12-31	not yet calculated	CVE-2018-6335 MISC MISC
hhvm -- hhvm	folly::secureRandom will re-use a buffer between parent and child processes when fork() is called. That will result in multiple forked children producing repeat (or similar) results. This affects HHVM 3.26 prior to 3.26.3 and the folly library between v2017.12.11.00 and v2018.08.09.00.	2018-12-31	not yet calculated	CVE-2018-6337 MISC MISC MISC
hhvm -- hhvm	Multipart-file uploads call variables to be improperly registered in the global scope. In cases where variables are not declared	2018-12-31	not yet	CVE-2018-6334

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	explicitly before being used this can lead to unexpected behavior. This affects all supported versions of HHVM prior to the patch (3.25.1, 3.24.5, and 3.21.9 and below).		calculated	MISC MISC
hsweb -- hsweb	A CSRF issue was discovered in web/authorization/oauth2/controller/OAuth2ClientController.java in hsweb 3.0.4 because the state parameter in the request is not compared with the state parameter in the session after user authentication is successful.	2018-12-30	not yet calculated	CVE-2018-20595 MISC MISC
hsweb -- hsweb	An issue was discovered in hsweb 3.0.4. It is a reflected XSS vulnerability due to the absence of type parameter checking in FlowableModelManagerController.java.	2018-12-30	not yet calculated	CVE-2018-20594 MISC MISC
huawei -- hg_products	There is an information leak vulnerability in some Huawei HG products. An attacker may obtain information about the HG device by exploiting this vulnerability.	2019-01-02	not yet calculated	CVE-2018-7900 CONFIRM MISC
imcat -- imcat	imcat 4.4 allows full path disclosure via a dev.php?tools-ipaddr&api=Pcoln&uip= URI.	2018-12-30	not yet calculated	CVE-2018-20606 MISC
imcat -- imcat	imcat 4.4 allows remote attackers to execute arbitrary PHP code by using root/run/adm.php to modify the boot/bootskip.php file.	2018-12-30	not yet calculated	CVE-2018-20605 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive debugging information via the root/tools/adbug/binfo.php URI.	2018-12-30	not yet calculated	CVE-2018-20607 MISC
imcat -- imcat	imcat 4.4 allows remote attackers to read phpinfo output via the root/tools/adbug/binfo.php?phpinfo1 URI.	2018-12-30	not yet calculated	CVE-2018-20608 MISC
imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive configuration information via the root/tools/adbug/check.php URI.	2018-12-30	not yet calculated	CVE-2018-20609 MISC
imcat -- imcat	imcat 4.4 allows directory traversal via the root/run/adm.php efile parameter.	2018-12-30	not yet calculated	CVE-2018-20610 MISC
imcat -- imcat	imcat 4.4 allow XSS via a crafted cookie to the root/tools/adbug/binfo.php?cookie URI.	2018-12-30	not yet calculated	CVE-2018-20611 MISC
inxedu -- inxedu	inxedu through 2018-12-24 has a SQL Injection vulnerability that can lead to information disclosure via the deleteFaveorite/ PATH_INFO. The vulnerable code location is com.inxedu.os.edu.controller.user.UserController#deleteFavorite (aka deleteFavorite in com/inxedu/os/edu/controller/user/UserController.java), where courseFavoritesService.deleteCourseFavoritesById is mishandled during use of MyBatis. NOTE: UserController.java has a	2019-01-02	not yet calculated	CVE-2019-3576 MISC

	spelling variation in an annotation: a @RequestMapping("/deleteFaveorite/{ids}") line followed by a "public ModelAndView deleteFavorite" line.			
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/add_pictures.php article ID.	2018-12-30	not yet calculated	CVE-2018-20589 MISC
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/users.php user ID.	2018-12-30	not yet calculated	CVE-2018-20590 MISC
jasper -- jasper	JasPer 2.0.14 has a memory leak in base/jas_malloc.c in libjasper.a when "--output-format jp2" is used.	2018-12-31	not yet calculated	CVE-2018-20622 BID MISC MLIST
jspxcms -- jspxcms	Jspxcms v9.0.0 allows SSRF.	2018-12-30	not yet calculated	CVE-2018-20596 MISC
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows full path disclosure via the /install.php?s=/1 URI.	2018-12-30	not yet calculated	CVE-2018-20602 MISC
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows admin.php?s=/Member/add.html CSRF.	2018-12-30	not yet calculated	CVE-2018-20603 MISC
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows Directory Traversal via crafted use	2018-12-30	not yet	CVE-2018-

	of ..* in Template/edit/path URIs, as demonstrated by the admin.php?s=/Template/edit/path/*web*..*..*..*..*1.txt.html URI to read the 1.txt file.		calculated	20604 MISC
libming -- libming	An issue was discovered in libming 0.4.8. There is a heap-based buffer over-read in the function writePNG in the file util/dbl2png.c of the dbl2png command-line program. Because this is associated with an erroneous call to png_write_row in libpng, an out-of-bounds write might occur for some memory layouts.	2019-01-02	not yet calculated	CVE-2019-3572 MISC
libsixel -- libsixel	In libsixel v1.8.2, there is a heap-based buffer over-read in the function load_jpeg() in the file loader.c, as demonstrated by img2sixel.	2019-01-02	not yet calculated	CVE-2019-3574 MISC MISC
libsixel -- libsixel	In libsixel v1.8.2, there is an infinite loop in the function sixel_decode_raw_impl() in the file fromsixel.c, as demonstrated by sixel2png.	2019-01-02	not yet calculated	CVE-2019-3573 MISC MISC
linux -- linux_kernel	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames. This is related to	2019-01-03	not yet calculated	CVE-2019-3701 BID MISC MISC

	cgw_csum_xor_rel. An unprivileged user can trigger a system crash (general protection fault).			
mcafee -- application_control_and_change_control	A whitelist bypass vulnerability in McAfee Application Control / Change Control 7.0.1 and before allows execution bypass, for example, with simple DLL through interpreters such as PowerShell.	2018-12-31	not yet calculated	CVE-2018-6668 CONFIRM
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is stack-based buffer overflow in the scan_file function in mxmldoc.c.	2018-12-30	not yet calculated	CVE-2018-20593 MISC MISC MISC
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is a use-after-free in the mxmlAdd function of the mxml-node.c file. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted xml file, as demonstrated by mxmldoc.	2018-12-30	not yet calculated	CVE-2018-20592 MISC MISC MISC
multiple_vendors -- multiple_products	An issue was discovered in osquery. A maliciously crafted Universal/fat binary can evade third-party code signing checks. By not completing full inspection of the Universal/fat binary, the user of the third-party tool will believe that the code is signed by Apple, but the malicious unsigned code will execute. This issue affects osquery prior to v3.2.7	2018-12-31	not yet calculated	CVE-2018-6336 MISC
mybb -- mybb	The OUGC Awards plugin before 1.8.19 for MyBB allows XSS via a crafted award reason that is mishandled on the awards page or in a user profile.	2019-01-02	not yet calculated	CVE-2019-3501

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

				MISC MISC
nuclide -- nuclide	The hhvm-attach deep link handler in Nuclide did not properly sanitize the provided hostname parameter when rendering. As a result, a malicious URL could be used to render HTML and other content inside of the editor's context, which could potentially be chained to lead to code execution. This issue affected Nuclide prior to v0.290.0.	2018-12-31	not yet calculated	CVE-2018-6333 MISC
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_csv_decode2 function in ok_csv.c.	2018-12-31	not yet calculated	CVE-2018-20617 MISC
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer over-read in the ok_mo_decode2 function in ok_mo.c.	2018-12-31	not yet calculated	CVE-2018-20618 MISC
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_wav_decode_ms_adpcm_data function in ok_wav.c.	2018-12-31	not yet calculated	CVE-2018-20616 MISC

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