GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Monday, December 10, 2018
GLESEC-CSFR0037

SB18-344: Vulnerability Summary for the Week of December 3, 2018
Original release date: December 10, 2018

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.

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

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

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
metinfo -- metinfo	Metinfo 6.1.3 has reflected XSS via the admin/column/move.php lang_columnerr4 parameter.	2018-12-03	4.3	CVE-2018-19835 MISC

Low Vulnerabilities

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

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

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- c1000a_router	Persistent Cross-Site Scripting (XSS) in the advancedsetup_websiteblocking.html Website Blocking page of the Actiontec C1000A router with firmware through CAC004-31.30L.95 allows a remote attacker to inject arbitrary HTML into the Website Blocking page by inserting arbitrary HTML into the 'TodUrlAdd' URL parameter in a /urlfilter.cmd POST request.	2018-12-06	not yet calculated	CVE-2018-19922 MISC
amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow information disclosure during parsing of ICMP packets in prvProcessICMPPacket.	2018-12-06	not yet calculated	CVE-2018-16527 MISC MISC CONFIRM
amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1 allows remote attackers to execute arbitrary code because of mbedTLS context object corruption in prvSetupConnection and	2018-12-06	not yet calculated	CVE-2018-16528 MISC MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	GGD_SecureConnect_Connect in AWS TLS connectivity modules.			
amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of DHCP responses in prvProcessDHCPReplies can be used for information disclosure.	2018-12-06	not yet calculated	CVE-2018-16602 MISC MISC CONFIRM
amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. A crafted IP header triggers a full memory space copy in prvProcessIPPacket, leading to denial of service and possibly remote code execution.	2018-12-06	not yet calculated	CVE-2018-16601 MISC MISC CONFIRM
amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of ARP packets in eARPProcessPacket can be used for information disclosure.	2018-12-06	not yet calculated	CVE-2018-16600 MISC MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. In xProcessReceivedUDPPacket and prvParseDNSReply, any received DNS response is accepted, without confirming it matches a sent DNS request.	2018-12-06	not yet calculated	CVE-2018-16598 MISC MISC CONFIRM
amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds memory access during parsing of NBNS packets in prvTreatNBNS can be used for information disclosure.	2018-12-06	not yet calculated	CVE-2018-16599 MISC MISC CONFIRM
amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow remote attackers to leak information or execute arbitrary code because of a Buffer Overflow during generation of a protocol checksum in usGenerateProtocolChecksum and prvProcessIPPacket.	2018-12-06	not yet calculated	CVE-2018-16526 MISC MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1 has an uninitialized pointer free in SOCKETS_SetSockOpt.	2018-12-06	not yet calculated	CVE-2018-16522 MISC MISC CONFIRM
amazon_web_services -- freertos	An issue was discovered in Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component. Out of bounds access to TCP source and destination port fields in xProcessReceivedTCPPacket can leak data back to an attacker.	2018-12-06	not yet calculated	CVE-2018-16603 MISC MISC CONFIRM
amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow remote attackers to execute arbitrary code or leak information because of a Buffer Overflow during parsing of DNS\LLMNR packets in prvParseDNSReply.	2018-12-06	not yet calculated	CVE-2018-16525 MISC MISC CONFIRM
amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow information disclosure during parsing of TCP options in prvCheckOptions.	2018-12-06	not yet calculated	CVE-2018-16524 MISC MISC CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

amazon_web_services -- freertos	Amazon Web Services (AWS) FreeRTOS through 1.3.1, FreeRTOS up to V10.0.1 (with FreeRTOS+TCP), and WITTENSTEIN WHIS Connect middleware TCP/IP component allow division by zero in prvCheckOptions.	2018-12-06	not yet calculated	CVE-2018-16523 MISC MISC CONFIRM
anker -- nebula_capsule_pro_nbui_m1_devices	Anker Nebula Capsule Pro NBUI_M1_V2.1.9 devices allow attackers to cause a denial of service (reboot of the underlying Android 7.1.2 operating system) via a crafted application that sends data to WifiService.	2018-12-08	not yet calculated	CVE-2018-19980 MISC
antiy_labs -- avl_atool	Local attackers can trigger a stack-based buffer overflow on vulnerable installations of Antiy-AVL ATool security management v1.0.0.22. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the processing of IOCTL 0x80002000 by the IRPFile.sys Antiy-AVL ATool kernel driver. The bug is caused by failure to properly validate the length of the user-supplied data, which results in a kernel stack buffer overflow. An attacker can leverage this vulnerability to execute arbitrary code in the context of the kernel, which could lead to privilege escalation and	2018-12-05	not yet calculated	CVE-2018-19650 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	a failed exploit could lead to denial of service.			
arm -- mbed_tls	Arm Mbed TLS before 2.14.1, before 2.7.8, and before 2.1.17 allows a local unprivileged attacker to recover the plaintext of RSA decryption, which is used in RSA-without-(EC)DH(E) cipher suites.	2018-12-05	not yet calculated	CVE-2018-19608 MISC CONFIRM CONFIRM
artifex -- mupdf	In Artifex MuPDF 1.14.0, svg/svg-run.c allows remote attackers to cause a denial of service (recursive calls followed by a fitz/xml.c fz_xml_att crash from excessive stack consumption) via a crafted svg file, as demonstrated by mupdf-gl.	2018-12-05	not yet calculated	CVE-2018-19881 MISC MISC
artifex -- mupdf	In Artifex MuPDF 1.14.0, the svg_run_image function in svg/svg-run.c allows remote attackers to cause a denial of service (href_att NULL pointer dereference and application crash) via a crafted svg file, as demonstrated by mupdf-gl.	2018-12-05	not yet calculated	CVE-2018-19882 MISC MISC
aruba -- access_points	A vulnerability exists in the firmware of embedded BLE radios that are part of some Aruba Access points. An attacker who is able to exploit the vulnerability could install new, potentially malicious firmware into the AP's BLE radio and could then gain access to the AP's console port. This vulnerability is applicable only if the BLE radio has been enabled in affected access points. The BLE radio	2018-12-07	not yet calculated	CVE-2018-7080 BID CONFIRM

	is disabled by default. Note - Aruba products are NOT affected by a similar vulnerability being tracked as CVE-2018-16986.			
aruba -- clearpass	A Remote Authentication bypass in Aruba ClearPass Policy Manager leads to complete cluster compromise. An authentication flaw in all versions of ClearPass could allow an attacker to compromise the entire cluster through a specially crafted API call. Network access to the administrative web interface is required to exploit this vulnerability. Resolution: Fixed in 6.7.6 and 6.6.10-hotfix.	2018-12-07	not yet calculated	CVE-2018-7067 CONFIRM
aruba -- clearpass	Aruba ClearPass Policy Manager guest authorization failure. Certain administrative operations in ClearPass Guest do not properly enforce authorization rules, which allows any authenticated administrative user to execute those operations regardless of privilege level. This could allow low-privilege users to view, modify, or delete guest users. Resolution: Fixed in 6.7.6 and 6.6.10-hotfix.	2018-12-07	not yet calculated	CVE-2018-7079 CONFIRM
aruba -- clearpass	An unauthenticated remote command execution exists in Aruba ClearPass Policy Manager on linked devices. The ClearPass OnConnect feature permits administrators to link other network devices into ClearPass for	2018-12-07	not yet calculated	CVE-2018-7066 CONFIRM

	the purpose of collecting enhanced information about connected endpoints. A defect in the API could allow a remote attacker to execute arbitrary commands on one of the linked devices. This vulnerability is only applicable if credentials for devices have been supplied to ClearPass under Configuration -> Network -> Devices -> CLI Settings. Resolution: Fixed in 6.7.5 and 6.6.10-hotfix.			
aruba -- clearpass	An authenticated SQL injection vulnerability in Aruba ClearPass Policy Manager can lead to privilege escalation. All versions of ClearPass are affected by multiple authenticated SQL injection vulnerabilities. In each case, an authenticated administrative user of any type could exploit this vulnerability to gain access to "appadmin" credentials, leading to complete cluster compromise. Resolution: Fixed in 6.7.6 and 6.6.10-hotfix.	2018-12-07	not yet calculated	CVE-2018-7065 CONFIRM
aruba -- clearpass	In Aruba ClearPass, disabled API admins can still perform read/write operations. In certain circumstances, API admins in ClearPass which have been disabled may still be able to perform read/write operations on parts of the XML API. This can lead to unauthorized access to the API and complete compromise of the	2018-12-07	not yet calculated	CVE-2018-7063 CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	ClearPass instance if an attacker knows of the existence of these accounts.			
asustor -- adm	Directory Traversal in downloadwallpaper.cgi in ASUSTOR ADM version 3.1.1 allows attackers to download arbitrary files by manipulating the "file" and "folder" URL parameters.	2018-12-04	not yet calculated	CVE-2018-12314 MISC
asustor -- adm	Missing verification of a password in ASUSTOR ADM version 3.1.1 allows attackers to change account passwords without entering the current password.	2018-12-04	not yet calculated	CVE-2018-12315 MISC
asustor -- adm	Denial-of-service in the login page of ASUSTOR ADM 3.1.1 allows attackers to prevent users from signing in by placing malformed text in the title.	2018-12-04	not yet calculated	CVE-2018-12319 MISC
asustor -- adm	OS command injection in user.cgi in ASUSTOR ADM version 3.1.1 allows attackers to execute system commands as root via the "secret_key" URL parameter.	2018-12-04	not yet calculated	CVE-2018-12312 MISC
asustor -- adm	Information disclosure in the SNMP settings page in ASUSTOR ADM version 3.1.1 allows attackers to obtain the SNMP password in cleartext.	2018-12-04	not yet calculated	CVE-2018-12318 MISC
asustor -- adm	OS command injection in group.cgi in ASUSTOR ADM version 3.1.1 allows attackers to execute system	2018-12-04	not yet calculated	CVE-2018-12317 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	commands as root by modifying the "name" POST parameter.			
asustor -- adm	OS Command Injection in upload.cgi in ASUSTOR ADM version 3.1.1 allows attackers to execute system commands by modifying the filename POST parameter.	2018-12-04	not yet calculated	CVE-2018-12316 MISC
asustor -- adm	Cross-site scripting in File Explorer in ASUSTOR ADM version 3.1.1 allows attackers to execute JavaScript by uploading SVG images with embedded JavaScript.	2018-12-04	not yet calculated	CVE-2018-12305 MISC
asustor -- adm	OS command injection in user.cgi in ASUSTOR ADM version 3.1.1 allows attackers to execute system commands as root via the "name" POST parameter.	2018-12-04	not yet calculated	CVE-2018-12307 MISC
asustor -- adm	Cross-site scripting vulnerability in File Explorer in ASUSTOR ADM version 3.1.1 allows attackers to execute arbitrary JavaScript when a file is moved via a malicious filename.	2018-12-04	not yet calculated	CVE-2018-12311 MISC
asustor -- adm	Cross-site scripting in the Login page in ASUSTOR ADM version 3.1.1 allows attackers to execute JavaScript via the System Announcement feature.	2018-12-04	not yet calculated	CVE-2018-12310 MISC
asustor -- adm	Directory Traversal in upload.cgi in ASUSTOR ADM version 3.1.1 allows attackers to upload files to arbitrary locations by modifying the "path" URL parameter. NOTE: the	2018-12-04	not yet calculated	CVE-2018-12309 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	"filename" POST parameter is covered by CVE-2018-11345.			
asustor -- adm	Encryption key disclosure in share.cgi in ASUSTOR ADM version 3.1.1 allows attackers to obtain the encryption key via the "encrypt_key" URL parameter.	2018-12-04	not yet calculated	CVE-2018-12308 MISC
asustor -- adm	Directory Traversal in File Explorer in ASUSTOR ADM version 3.1.1 allows attackers to view arbitrary files by modifying the "file1" URL parameter, a similar issue to CVE-2018-11344.	2018-12-04	not yet calculated	CVE-2018-12306 MISC
asustor -- adm	OS command injection in snmp.cgi in ASUSTOR ADM version 3.1.1 allows attackers to execute system commands without authentication via the "rocommunity" URL parameter.	2018-12-04	not yet calculated	CVE-2018-12313 MISC
bastian_allgeier -- kirby	panel/login in Kirby v2.5.12 allows XSS via a blog name.	2018-12-04	not yet calculated	CVE-2018-16628 MISC
brocade_communications -- fabric_os	A vulnerability in the proxy service of Brocade Fabric OS versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow remote unauthenticated attackers to obtain sensitive information and possibly cause a denial of service attack.	2018-12-03	not yet calculated	CVE-2018-6440 CONFIRM
brocade_communications -- fabric_os	A vulnerability in the configdownload command of Brocade Fabric OS command line interface (CLI) versions before 8.2.1, 8.1.2f, 8.0.2f, 7.4.2d could allow a	2018-12-03	not yet calculated	CVE-2018-6439 CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

	local attacker to escape the restricted shell and, gain root access.			
cairo -- cairo	cairo 1.16.0, in cairo_ft_apply_variations() in cairo-ft-font.c, would free memory using a free function incompatible with WebKit's fastMalloc, leading to an application crash with a "free(): invalid pointer" error.	2018-12-05	not yet calculated	CVE-2018-19876 MISC MISC
chipsbank_technologies -- ump_tool	ChipsBank UMPTool saves the password to the NAND with a simple substitution cipher, which allows attackers to get full access when having physical access to the device.	2018-12-03	not yet calculated	CVE-2018-19795 MISC
cisco -- energy_management_suite	A vulnerability in the configuration of a local database installed as part of the Cisco Energy Management Suite (CEMS) could allow an authenticated, local attacker to access and alter confidential data. The vulnerability is due to the installation of the PostgreSQL database with unchanged default access credentials. An attacker could exploit this vulnerability by logging in to the machine where CEMS is installed and establishing a local connection to the database. The fix for this vulnerability randomizes the database access password in new installations; however, the fix will not change the password for existing installations. Users are required to manually change the password, as documented	2018-12-04	not yet calculated	CVE-2018-0468 BID CISCO MISC

	in the Workarounds section of this advisory. There are workarounds that address this vulnerability.			
cloud_foundry -- cloud_foundry_nfs	Cloud Foundry NFS volume release, 1.2.x prior to 1.2.5, 1.5.x prior to 1.5.4, 1.7.x prior to 1.7.3, logs the cf admin username and password when running the nfsbrokerpush BOSH deploy errand. A remote authenticated user with access to BOSH can obtain the admin credentials for the Cloud Foundry Platform through the logs of the NFS volume deploy errand.	2018-12-05	not yet calculated	CVE-2018-15797 CONFIRM
crafter_software -- crafter_cms	A Server-Side Template Injection issue was discovered in Crafter CMS 3.0.18. Attackers with developer privileges may execute OS commands by Creating/Editing a template file (.ftl filetype) that triggers a call to freemarker.template.utility.Execute in the FreeMarker library during rendering of a web page.	2018-12-06	not yet calculated	CVE-2018-19907 MISC MISC
dell -- encryption	Dell Encryption (formerly Dell Data Protection | Encryption) v10.1.0 and earlier contain an information disclosure vulnerability. A malicious user with physical access to the machine could potentially exploit this vulnerability to access the unencrypted RegBack folder that contains back-ups of sensitive system files.	2018-12-05	not yet calculated	CVE-2018-15773 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

domainmod -- domainmod	DomainMOD through 4.11.01 has XSS via the assets/add/registrar-accounts.php UserName, Reseller ID, or notes field.	2018-12-06	not yet calculated	CVE-2018-19913 MISC
domainmod -- domainmod	DomainMOD through 4.11.01 has XSS via the assets/add/dns.php Profile Name or notes field.	2018-12-06	not yet calculated	CVE-2018-19914 MISC
domainmod -- domainmod	DomainMOD through 4.11.01 has XSS via the assets/edit/host.php Web Host Name or Web Host URL field.	2018-12-06	not yet calculated	CVE-2018-19915 MISC
domainmod -- domainmod	DomainMOD through 4.11.01 has XSS via the admin/dw/add-server.php DisplayName, HostName, or UserName field.	2018-12-05	not yet calculated	CVE-2018-19892 MISC
drobo -- 5n2_nas	Incorrect access control in the /mysql/api/diags.php endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to retrieve diagnostic information via the "name" URL parameter.	2018-12-03	not yet calculated	CVE-2018-14695 MISC
drobo -- 5n2_nas	Incorrect access control in the /mysql/api/drobo.php endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to retrieve sensitive system information.	2018-12-03	not yet calculated	CVE-2018-14696 MISC
drobo -- 5n2_nas	Cross-site scripting in the /DroboAccess/enable_user endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows attackers to execute JavaScript via the username URL parameter.	2018-12-03	not yet calculated	CVE-2018-14697 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

drobo -- 5n2_nas	Cross-site scripting in the /DroboAccess/delete_user endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows attackers to execute JavaScript via the "username" URL parameter.	2018-12-03	not yet calculated	CVE-2018-14698 MISC
drobo -- 5n2_nas	System command injection in the /DroboAccess/enable_user endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to execute system commands via the "username" URL parameter.	2018-12-03	not yet calculated	CVE-2018-14699 MISC
drobo -- 5n2_nas	Incorrect access control in the /mysql/api/droboapp/data endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to retrieve the MySQL database root password.	2018-12-03	not yet calculated	CVE-2018-14703 MISC
drobo -- 5n2_nas	System command injection in the /DroboAccess/delete_user endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to execute system commands via the "username" URL parameter.	2018-12-03	not yet calculated	CVE-2018-14701 MISC
drobo -- 5n2_nas	Incorrect access control in the /dropopix/api/drobo.php endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to retrieve sensitive system information.	2018-12-03	not yet calculated	CVE-2018-14702 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

drobo -- 5n2_nas	Incorrect access control in the Dashboard API on Drobo 5N2 NAS version 4.0.5-13.28.96115 allows attackers to bypass authentication due to insecure token generation.	2018-12-03	not yet calculated	CVE-2018-14709 MISC
drobo -- 5n2_nas	An insecure transport protocol used by Drobo Dashboard API on Drobo 5N2 NAS version 4.0.5-13.28.96115 allows attackers to intercept network traffic.	2018-12-03	not yet calculated	CVE-2018-14708 MISC
drobo -- 5n2_nas	Directory traversal in the Drobo Pix web application on Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to upload files to arbitrary locations.	2018-12-03	not yet calculated	CVE-2018-14707 MISC
drobo -- 5n2_nas	System command injection in the /DroboPix/api/drobopix/demo endpoint on Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to execute system commands via the payload in a POST request.	2018-12-03	not yet calculated	CVE-2018-14706 MISC
drobo -- 5n2_nas	Incorrect access control in the /mysql/api/logfile.php endpoint in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows unauthenticated attackers to retrieve MySQL log files via the "name" URL parameter.	2018-12-03	not yet calculated	CVE-2018-14700 MISC
drobo -- 5n2_nas	Cross-site scripting in the MySQL API error page in Drobo 5N2 NAS version 4.0.5-13.28.96115 allows attackers to execute JavaScript via a malformed URL path.	2018-12-03	not yet calculated	CVE-2018-14704 MISC

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

f5 -- big-ip	The svpn component of the F5 BIG-IP APM client prior to version 7.1.7.2 for Linux and macOS runs as a privileged process and can allow an unprivileged user to get ownership of files owned by root on the local client host in a race condition.	2018-12-06	not yet calculated	CVE-2018-15332 BID CONFIRM
foreman -- foreman	A cross-site scripting (XSS) flaw was found in the foreman component of satellite. An attacker with privilege to create entries using the Hosts, Monitor, Infrastructure, or Administer Menus is able to execute a XSS attacks against other users, possibly leading to malicious code execution and extraction of the anti-CSRF token of higher privileged users. Foreman before 1.18.3, 1.19.1, and 1.20.0 are vulnerable.	2018-12-07	not yet calculated	CVE-2018-16861 CONFIRM
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r340854) and 11.2-RELEASE-p5, an integer overflow error when handling opcodes can cause memory corruption by sending a specially crafted NFSv4 request. Unprivileged remote users with access to the NFS server may be able to execute arbitrary code.	2018-12-04	not yet calculated	CVE-2018-17157 SECTRACK MISC FREEBSD
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r340854) and 11.2-RELEASE-p5, an integer overflow error can occur when handling the client address length field in an NFSv4 request. Unprivileged remote	2018-12-04	not yet calculated	CVE-2018-17158 SECTRACK MISC FREEBSD

	users with access to the NFS server can crash the system by sending a specially crafted NFSv4 request.			
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r340854) and 11.2-RELEASE-p5, the NFS server lacks a bounds check in the READDIRPLUS NFS request. Unprivileged remote users with access to the NFS server can cause a resource exhaustion by forcing the server to allocate an arbitrarily large memory allocation.	2018-12-04	not yet calculated	CVE-2018-17159 SECTRACK MISC FREEBSD
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r341486) and 11.2-RELEASE-p6, insufficient bounds checking in one of the device models provided by bhyve can permit a guest operating system to overwrite memory in the bhyve host possibly permitting arbitrary code execution. A guest OS using a firmware image can cause the bhyve process to crash, or possibly execute arbitrary code on the host as root.	2018-12-04	not yet calculated	CVE-2018-17160 FREEBSD
freeswitch -- freeswitch	FreeSWITCH through 1.8.2, when mod_xml_rpc is enabled, allows remote attackers to execute arbitrary commands via the api/system or txtapi/system (or api/bg_system or txtapi/bg_system) query string on TCP port 8080, as demonstrated by an api/system?calc URI. This can also be exploited via CSRF. Alternatively, the default password of works for the freeswitch account can sometimes be used.	2018-12-06	not yet calculated	

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

GLESEC CYBER SECURITY FLASH REPORT

TLP-WHITE

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

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