GLESEC CYBER SECURITY FLASH REPORT

TLP-GREEN

Tuesday, April 24, 2018
GLESEC-CSFR0003

SB18-113: Vulnerability Summary for the Week of April 16, 2018

04/23/2018 06:32 AM EDT

Original release date: April 23, 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.

High Vulnerabilities

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

Medium Vulnerabilities

GLESEC CYBER SECURITY FLASH REPORT

TLP-GREEN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cms_made_simple	CMS Made Simple (CMSMS) through 2.2.6 contains an admin password reset vulnerability because data values are improperly compared, as demonstrated by a hash beginning with the "0e" substring.	2018-04-13	5.0	CVE-2018-10081 MISC

Low Vulnerabilities

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

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
7-zip--7-zip	7-Zip through 18.01 on Windows implements the "Large memory pages" option by calling the LsaAddAccountRights function to add the SeLockMemoryPrivilege privilege to the user's account, which makes it easier for attackers to bypass intended access restrictions by using this privilege in the context of a sandboxed process.	2018-04-16	not yet calculated	CVE-2018-10172 MISC
Adaltech--adaltech_g-ticket	Adaltech G-Ticket v70 EME104 has SQL Injection via the mobile-loja/mensagem.asp eve_cod parameter.	2018-04-21	not yet calculated	CVE-2018-10284 MISC
Apache--fineract	Apache Fineract 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating exposes	2018-04-20	not yet calculated	CVE-2018-1291

	different REST end points to query domain specific entities with a Query Parameter 'orderBy' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' query parameter by way of the "order" param in such a way to read/update the data for which he doesn't have authorization.			MLIST
Apache--fineract	Within the 'getReportType' method in Apache Fineract 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating, a hacker could inject SQL to read/update data for which he doesn't have authorization for by way of the 'reportName' parameter.	2018-04-20	not yet calculated	CVE-2018-1292 MLIST
Apache--fineract	In Apache Fineract versions 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating, the system exposes different REST end points to query domain specific entities with a Query Parameter 'orderBy' and 'sortOrder' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' and 'sortOrder' query parameter in such a way to read/update the data for which he doesn't have authorization.	2018-04-20	not yet calculated	CVE-2018-1289 MLIST
Apache--fineract	In Apache Fineract versions 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating, Using a single quotation escape with two continuous SQL parameters can cause a SQL injection. This could be done in Methods like retrieveAuditEntries of AuditsApiResource Class and retrieveCommands of MakercheckersApiResource Class.	2018-04-20	not yet calculated	CVE-2018-1290 MLIST
Apache-wicket-jquery-ui	In Apache wicket-jquery-ui <= 6.29.0, <= 7.10.1, <= 8.0.0-M9.1, JS code created in WYSIWYG editor will be executed on	2018-04-18	not yet calculated	CVE-2018-1325 MLIST

	display.			
appear_tv--xc5000_and_xc5100_devices	On Appear TV XC5000 and XC5100 devices with firmware 3.26.217, it is possible to read OS files with a specially crafted HTTP request (such as GET /../../../../../../../../../../../../etc/passwd) to the web server (fuzzd/0.1.1) running the Maintenance Center on port TCP/8088. This can lead to full compromise of the device.	2018-04-17	not yet calculated	CVE-2018-7539 FULLDISC
Artifex-ghostscript	The set_text_distance function in devices/vector/gdevpdts.c in the pdfwrite component in Artifex Ghostscript through 9.22 does not prevent overflows in text-positioning calculation, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.	2018-04-18	Not yet calculated	CVE-2018-10194 MISC SECTRACK MISC
Asus-multiple_routers	ASUS RT-AC51U, RT-AC58U, RT-AC66U, RT-AC1750, RT-ACRH13, and RT-N12 D1 routers with firmware before 3.0.0.4.380.8228; RT-AC52U B1, RT-AC1200 and RT-N600 routers with firmware before 3.0.0.4.380.10446; RT-AC55U and RT-AC55UHP routers with firmware before 3.0.0.4.382.50276; RT-AC86U and RT-AC2900 routers with firmware before 3.0.0.4.384.20648; and possibly other RT-series routers allow remote attackers to execute arbitrary code via unspecified vectors.	2018-04-20	not yet calculated	CVE-2018-8826 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
Atlassian-atlassian-renderer	The wiki markup component of atlassian-renderer from version 8.0.0 before version 8.0.22 allows remote attackers to inject	2018-04-17	not yet calculated	CVE-2017-18102 CONFIRM

GLESEC CYBER SECURITY FLASH REPORT

TLP-GREEN

	arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in nested wiki markup.			CONFIRM
Awstats-awstats	A Full Path Disclosure vulnerability in AWStats through 7.6 allows remote attackers to know where the config file is allocated, obtaining the full path of the server, a similar issue to CVE-2006-3682. The attack can, for example, use the awstats.pl framename and update parameters.	2018-04-20	not yet calculated	CVE-2018-10245 MISC
Bacnet-protocol_stack	bvlc.c in skarg BACnet Protocol Stack 0.8.5 has a buffer overflow in BACnet/IP BVLC packet processing because of a lack of packet-size validation.	2018-04-20	not yet calculated	CVE-2018-10238 CONFIRM
Baijiacms-baijiacms	baijiacms V3 has CSRF via index.php?mod=site&op=edituser&name=manager&do=user to add an administrator account.	2018-04-20	not yet calculated	CVE-2018-10249 MISC
baijiacms baijiacms	baijiacms V3 has physical path leakage via an index.php?mod=mobile&name=member&do=index request.	2018-04-19	not yet calculated	CVE-2018-10219 MISC
beescms - beescms	BEESCMS 4.0 has a CSRF vulnerability to add an administrator account via the admin/admin_admin.php?nav=list_admin_user&admin_p_nav=user URI.	2018-04-21	not yet calculated	CVE-2018-10266 MISC
belkin - belkin_n750_router	A remote unauthenticated user can execute commands as root in the Belkin N750 using firmware version 1.10.22 by sending a crafted HTTP request to proxy.cgi.	2018-04-19	not yet calculated	CVE-2018-1144 MISC
Belkin - belkin_n750_router	A remote unauthenticated user can execute commands as root in the Belkin N750 using firmware version 1.10.22 by sending a crafted HTTP request to twonky_command.cgi.	2018-04-19	not yet calculated	CVE-2018-1143 MISC

belkin - belkin_n750_router	A remote unauthenticated user can overflow a stack buffer in the Belkin N750 using firmware version 1.10.22 by sending a crafted HTTP request to proxy.cgi.	2018-04-19	not yet calculated	CVE-2018-1145 MISC
belkin - belkin_n750_router	A remote unauthenticated user can enable telnet on the Belkin N750 using firmware version 1.10.22 by sending a crafted HTTP request to set.cgi. When enabled the telnet session requires no password and provides root access.	2018-04-19	Not yet calculated	CVE-2018-1146 MISC
bigtree - bigtree	An issue was discovered in BigTree 4.2.22. There is cross-site scripting (XSS) in /core/inc/lib/less.php/test/index.php because of a $_SERVER['REQUEST_URI'] echo, as demonstrated by the dir parameter in a file=charsets action.	2018-04-17	not yet calculated	CVE-2018-10183 MISC
bmc_medical_and_3b_medical - luna_cpap_machine	BMC Medical Luna CPAP Machines released prior to July 1, 2017, contain an improper input validation vulnerability which may allow an authenticated attacker to crash the CPAP's Wi-Fi module resulting in a denial-of-service condition.	2018-04-17	not yet calculated	CVE-2017-12701 BID MISC
cisco - adaptive_security_appliance_and_firepower_threat_defense	A vulnerability in the Transport Layer Security (TLS) library of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of the affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a malicious TLS message to an interface enabled for Secure Layer Socket (SSL) services on an affected device. Messages using SSL Version 3 (SSLv3) or SSL Version 2 (SSLv2) cannot be	2018-04-19	Not yet calculated	CVE-2018-0231 SECTRACK CONFIRM

	be used to exploit this vulnerability. An exploit could allow the attacker to cause a buffer underflow, triggering a crash on an affected device. This vulnerability affects Cisco ASA Software and Cisco FTD Software that is running on the following Cisco products: Adaptive Security Virtual Appliance (ASAv), Firepower Threat Defense Virtual (FTDv), Firepower 2100 Series Security Appliance. Cisco Bug IDs: CSCve18902, CSCve34335, CSCve38446.			
cisco - adaptive_security_appliance_and_firepower_threat_defense	Multiple vulnerabilities in the Application Layer Protocol Inspection feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerabilities are due to logical errors during traffic inspection. An attacker could exploit these vulnerabilities by sending a high volume of malicious traffic across an affected device. An exploit could allow the attacker to cause a deadlock condition, resulting in a reload of an affected device. These vulnerabilities affect Cisco ASA Software and Cisco FTD Software configured for Application Layer Protocol Inspection running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4100 Series Security	2018-04-19	not yet calculated	CVE-2018-0240 BID SECTRACK CONFIRM

	Appliance, Firepower 9300 ASA Security Module, FTD Virtual (FTDv). Cisco Bug IDs: CSCve61540, CSCvh23085, CSCvh95456.			
cisco - adaptive_security_appliance	A vulnerability in the WebVPN web-based management interface of Cisco Adaptive Security Appliance could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCvg33985.	2018-04-19	Not yet calculated	CVE-2018-0242 BID SECTRAC K CONFIRM
cisco - adaptive_security_appliance	A vulnerability in the Web Server Authentication Required screen of the Clientless Secure Sockets Layer (SSL) VPN portal of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of that portal on an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the portal or allow the attacker to access	2018-04-19	not yet calculated	CVE-2018-0251 BID SECTRAC K CONFIRM

	sensitive browser-based information. This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco ASA Software: 3000 Series Industrial Security Appliances, Adaptive Security Virtual Appliance (ASAv), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches, ASA Services Module for Cisco 7600 Series Routers. Cisco Bug IDs: CSCvh20742.			
cisco - adaptive_security_appliance	A vulnerability in the Secure Sockets Layer (SSL) Virtual Private Network (VPN) Client Certificate Authentication feature for Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, remote attacker to establish an SSL VPN connection and bypass certain SSL certificate verification steps. The vulnerability is due to incorrect verification of the SSL Client Certificate. An attacker could exploit this vulnerability by connecting to the ASA VPN without a proper private key and certificate pair. A successful exploit could allow the attacker to establish an SSL VPN connection to the ASA when the connection should have been rejected. This vulnerability affects Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software that is running on the following Cisco products: 3000 Series Industrial Security Appliances (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Adaptive Security Virtual Appliances (ASAv), Firepower 4110	2018-04-19	not yet calculated	CVE-2018-0227 SECTRACK CONFIRM

	Security Appliances, Firepower 9300 ASA Security Modules. Cisco Bug IDs: CSCvg40155.			
cisco - adaptive_security_appliance	A vulnerability in the ingress flow creation functionality of Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, remote attacker to cause the CPU to increase upwards of 100% utilization, causing a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect handling of an internal software lock that could prevent other system processes from getting CPU cycles, causing a high CPU condition. An attacker could exploit this vulnerability by sending a steady stream of malicious IP packets that can cause connections to be created on the targeted device. A successful exploit could allow the attacker to exhaust CPU resources, resulting in a DoS condition during which traffic through the device could be delayed. This vulnerability applies to either IPv4 or IPv6 ingress traffic. This vulnerability affects Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software that is running on the following Cisco products: 3000 Series Industrial Security Appliances (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Adaptive Security Virtual Appliances (ASAv), Firepower 2100 Series Security Appliances, Firepower 4110 Security Appliances, Firepower 9300 ASA Security Modules. Cisco Bug IDs: CSCvf63718.	2018-04-19	not yet calculated	CVE-2018-0228 SECTRACK CONFIRM

cisco - advanced_malware_protection_for_endpoints_macos_connector	A vulnerability in the file type detection mechanism of the Cisco Advanced Malware Protection (AMP) for Endpoints macOS Connector could allow an unauthenticated, remote attacker to bypass malware detection. The vulnerability occurs because the software relies on only the file extension for detecting DMG files. An attacker could exploit this vulnerability by sending a DMG file with a nonstandard extension to a device that is running an affected AMP for Endpoints macOS Connector. An exploit could allow the attacker to bypass configured malware detection. Cisco Bug IDs: CSCve34034.	2018-04-19	not yet calculated	CVE-2018-0237 CONFIRM
cisco - digital_network_architecture_center	A vulnerability in the web framework of the Cisco Digital Network Architecture Center (DNA Center) could allow an unauthenticated, remote attacker to communicate with the Kong API server without restriction. The vulnerability is due to an overly permissive Cross Origin Resource Sharing (CORS) policy. An attacker could exploit this vulnerability by convincing a user to follow a malicious link. An exploit could allow the attacker to communicate with the API and exfiltrate sensitive information. Cisco Bug IDs: CSCvh99208.	2018-04-19	not yet calculated	CVE-2018-0269 CONFIRM
	A vulnerability in the Secure Sockets Layer (SSL) packet reassembly functionality of the detection engine in Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause the detection engine to consume excessive system memory on an affected device, which could cause a denial of service (DoS) condition. The vulnerability			

cisco - firepower_system_ software	is due to the affected software improperly handling changes to SSL connection states. An attacker could exploit this vulnerability by sending crafted SSL connections through an affected device. A successful exploit could allow the attacker to cause the detection engine to consume excessive system memory on the affected device, which could cause a DoS condition. The device may need to be reloaded manually to recover from this condition. This vulnerability affects Cisco Firepower System Software Releases 6.0.0 and later, running on any of the following Cisco products: Adaptive Security Appliance (ASA) 5500-X Series Firewalls with FirePOWER Services, Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls, Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances, Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances, Firepower 4100 Series Appliances, FirePOWER 7000 Series Appliances, FirePOWER 8000 Series Appliances, Firepower 9300 Series Security Appliances, Firepower Threat Defense for Integrated Services Routers (ISRs), Firepower Threat Defense Virtual for VMware, Industrial Security Appliance 3000, Sourcefire 3D System Appliances. Cisco Bug IDs: CSCve23031.	2018-04-19	not yet calculated	CVE-2018-0233 BID CONFIRM
cisco - firepower_system_ software	A vulnerability in the Secure Sockets Layer (SSL) Engine of Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper error handling while processing SSL traffic. An attacker could exploit this	2018-04-19	not yet calculated	CVE-2018-0272 BID CONFIRM

	vulnerability by sending a large volume of crafted SSL traffic to the vulnerable device. A successful exploit could allow the attacker to degrade the device performance by triggering a persistent high CPU utilization condition. Cisco Bug IDs: CSCvh89340.			
cisco - firepower_system_ software	A vulnerability in the detection engine of Cisco Firepower System Software could allow an unauthenticated, remote attacker to bypass configured file action policies if an Intelligent Application Bypass (IAB) with a drop percentage threshold is also configured. The vulnerability is due to incorrect counting of the percentage of dropped traffic. An attacker could exploit this vulnerability by sending network traffic to a targeted device. An exploit could allow the attacker to bypass configured file action policies, and traffic that should be dropped could be allowed into the network. Cisco Bug IDs: CSCvf86435.	2018-04-19	not yet calculated	CVE-2018-0254 CONFIRM
cisco - firepower_system_ software	A vulnerability in the detection engine of Cisco Firepower System Software could allow an unauthenticated, remote attacker to bypass a configured file action policy to drop the Server Message Block (SMB) protocol if a malware file is detected. The vulnerability is due to how the SMB protocol handles a case in which a large file transfer fails. This case occurs when some pieces of the file are successfully transferred to the remote endpoint, but ultimately the file transfer fails and is reset. An attacker could exploit this vulnerability by sending a crafted SMB file transfer request through the targeted device. An exploit could allow the attacker to pass an SMB file that contains malware, which the device is configured to block. This	2018-04-19	not yet calculated	CVE-2018-0244 CONFIRM

	vulnerability affects Cisco Firepower System Software when one or more file action policies are configured, on software releases prior to 6.2.3. Cisco Bug IDs: CSCvc20141.			
cisco - firepower_system_software	A vulnerability in the detection engine of Cisco Firepower System Software could allow an unauthenticated, remote attacker to bypass a configured file action policy that is intended to drop the Server Message Block Version 2 (SMB2) and SMB Version 3 (SMB3) protocols if malware is detected. The vulnerability is due to incorrect detection of an SMB2 or SMB3 file based on the total file length. An attacker could exploit this vulnerability by sending a crafted SMB2 or SMB3 transfer request through the targeted device. An exploit could allow the attacker to pass SMB2 or SMB3 files that could be malware even though the device is configured to block them. This vulnerability does not exist for SMB Version 1 (SMB1) files. This vulnerability affects Cisco Firepower System Software when one or more file action policies are configured, on software releases prior to 6.2.3. Cisco Bug IDs: CSCvg68807.	2018-04-19	not yet calculated	CVE-2018-0243 CONFIRM
cisco - firepower_threat_defense_software_for_cisco_firepower_2100_series_security_appliances	A vulnerability in the internal packet-processing functionality of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Security Appliances could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to the affected software improperly validating IP Version 4 (IPv4) and IP Version 6 (IPv6) packets after the software	2018-04-19	not yet calculated	CVE-2018-0230 BID CONFIRM

	reassembles the packets (following IP Fragmentation). An attacker could exploit this vulnerability by sending a series of malicious, fragmented IPv4 or IPv6 packets to an affected device. A successful exploit could allow the attacker to cause Snort processes on the affected device to hang at 100% CPU utilization, which could cause the device to stop processing traffic and result in a DoS condition until the device is reloaded manually. This vulnerability affects Cisco Firepower Threat Defense (FTD) Software Releases 6.2.1 and 6.2.2, if the software is running on a Cisco Firepower 2100 Series Security Appliance. Cisco Bug IDs: CSCvf91098.			
cisco - identity_services_engine	A vulnerability in the support tunnel feature of Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to access the device's shell. The vulnerability is due to improper configuration of the support tunnel feature. An attacker could exploit this vulnerability by tricking the device into unlocking the support user account and accessing the tunnel password and device serial number. A successful exploit could allow the attacker to run any system command with root access. This affects Cisco Identity Services Engine (ISE) software versions prior to 2.2.0.470. Cisco Bug IDs: CSCvf54409.	2018-04-19	not yet calculated	CVE-2018-0275 SECTRAC K CONFIRM
cisco - industrial_ethernet_switches	A vulnerability in the device manager web interface of Cisco Industrial Ethernet Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user	2018-04-19	not yet calculated	CVE-2018-0255 SECTRAC K CONFIRM

	of an affected system. The vulnerability is due to insufficient CSRF protection by the device manager web interface. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link or visit an attacker-controlled website. A successful exploit could allow the attacker to submit arbitrary requests to an affected device via the device manager web interface with the privileges of the user. This vulnerability affects the following Cisco Industrial Ethernet (IE) Switches if they are running a vulnerable release of Cisco IOS Software: IE 2000 Series, IE 2000U Series, IE 3000 Series, IE 3010 Series, IE 4000 Series, IE 4010 Series, IE 5000 Series. Cisco Bug IDs: CSCvc96405.			
cisco - ios_xe_software	A vulnerability in Cisco IOS XE Software running on Cisco cBR Series Converged Broadband Routers could allow an unauthenticated, adjacent attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to the incorrect handling of certain DHCP packets. An attacker could exploit this vulnerability by sending certain DHCP packets to a specific segment of an affected device. A successful exploit could allow the attacker to increase CPU usage on the affected device and cause a DoS condition. Cisco Bug IDs: CSCvg73687.	2018-04-19	not yet calculated	CVE-2018-0257 SECTRAC K CONFIRM
cisco - ios_xr_software	A vulnerability in the UDP broadcast forwarding function of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the affected device. The	2018-04-19	not yet calculated	CVE-2018-0241 BID SECTRAC K

	vulnerability is due to improper handling of UDP broadcast packets that are forwarded to an IPv4 helper address. An attacker could exploit this vulnerability by sending multiple UDP broadcast packets to the affected device. An exploit could allow the attacker to cause a buffer leak on the affected device, eventually resulting in a DoS condition requiring manual intervention to recover. This vulnerability affects all Cisco IOS XR platforms running 6.3.1, 6.2.3, or earlier releases of Cisco IOS XR Software when at least one IPv4 helper address is configured on an interface of the device. Cisco Bug IDs: CSCvi35625.			CONFIRM
cisco - mate_collector	A vulnerability in the web-based management interface of Cisco MATE Collector could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions on a targeted device via a web browser and with the privileges of the user. Cisco Bug IDs: CSCvh31222.	2018-04-19	not yet calculated	CVE-2018-0259 BID CONFIRM
cisco - mate_live	A vulnerability in the web interface of Cisco MATE Live could allow an unauthenticated, remote attacker to view and download the contents of certain web application virtual directories. The vulnerability is due to lack of proper input validation and authorization of	2018-04-19	not yet calculated	CVE-2018-0260 CONFIRM

	HTTP requests. An attacker could exploit this vulnerability by sending a malicious HTTP request to the targeted application. An exploit could allow the attacker to view sensitive information that should require authentication. Cisco Bug IDs: CSCvh31272.			
cisco - multiple_products	A vulnerability in the IPsec Manager of Cisco StarOS for Cisco Aggregation Services Router (ASR) 5000 Series Routers and Virtualized Packet Core (VPC) System Software could allow an unauthenticated, remote attacker to terminate all active IPsec VPN tunnels and prevent new tunnels from being established, resulting in a denial of service (DoS) condition. The vulnerability is due to improper processing of corrupted Internet Key Exchange Version 2 (IKEv2) messages. An attacker could exploit this vulnerability by sending crafted IKEv2 messages toward an affected router. A successful exploit could allow the attacker to cause the ipsecmgr service to reload. A reload of this service could cause all IPsec VPN tunnels to be terminated and prevent new tunnels from being established until the service has restarted, resulting in a DoS condition. This vulnerability affects the following Cisco products when they are running Cisco StarOS: Cisco Aggregation Services Router (ASR) 5000 Series Routers, Virtualized Packet Core (VPC) System Software. Cisco Bug IDs: CSCve29605.	2018-04-19	not yet calculated	CVE-2018-0273 BID SECTRAC K CONFIRM
cisco - multiple_products	A vulnerability in Cisco WebEx Business Suite clients, Cisco WebEx Meetings, and Cisco WebEx Meetings Server could allow an authenticated, remote attacker to execute arbitrary code on a targeted system. The	2018-04-19	not yet calculated	CVE-2018-0112 BID SECTRAC K

	vulnerability is due to insufficient input validation by the Cisco WebEx clients. An attacker could exploit this vulnerability by providing meeting attendees with a malicious Flash (.swf) file via the file-sharing capabilities of the client. Exploitation of this vulnerability could allow arbitrary code execution on the system of a targeted user. This affects the clients installed by customers when accessing a WebEx meeting. The following client builds of Cisco WebEx Business Suite (WBS30, WBS31, and WBS32), Cisco WebEx Meetings, and Cisco WebEx Meetings Server are impacted: Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.2, Cisco WebEx Business Suite (WBS32) client builds prior to T32.10, Cisco WebEx Meetings with client builds prior to T32.10, Cisco WebEx Meetings Server builds prior to 2.8 MR2. Cisco Bug IDs: CSCvg19384, CSCvi10746.			CONFIRM
cisco - multiple_products	A vulnerability in the implementation of Security Assertion Markup Language (SAML) Single Sign-On (SSO) authentication for Cisco AnyConnect Secure Mobility Client for Desktop Platforms, Cisco Adaptive Security Appliance (ASA) Software, and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to establish an authenticated AnyConnect session through an affected device running ASA or FTD Software. The authentication would need to be done by an unsuspecting third party, aka Session Fixation. The vulnerability exists because there is no mechanism for the ASA or FTD Software to detect that the authentication request originates from the	2018-04-19	not yet calculated	CVE-2018-0229 SECTRAC K SECTRAC K CONFIRM

	AnyConnect client directly. An attacker could exploit this vulnerability by persuading a user to click a crafted link and authenticating using the company's Identity Provider (IdP). A successful exploit could allow the attacker to hijack a valid authentication token and use that to establish an authenticated AnyConnect session through an affected device running ASA or FTD Software. This vulnerability affects the Cisco AnyConnect Secure Mobility Client, and ASA Software and FTD Software configured for SAML 2.0-based SSO for AnyConnect Remote Access VPN that is running on the following Cisco products: 3000 Series Industrial Security Appliances (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4100 Series Security Appliance, Firepower 9300 ASA Security Module, FTD Virtual (FTDv). Cisco Bug IDs: CSCvg65072, CSCvh87448.			
cisco - packet_data_network_gateway	A vulnerability in the peer-to-peer message processing functionality of Cisco Packet Data Network Gateway could allow an unauthenticated, remote attacker to cause the Session Manager (SESSMGR) process on an affected device to restart, resulting in a denial of service (DoS) condition. The vulnerability is due to incorrect validation of peer-to-peer packet headers. An attacker could exploit this vulnerability by sending a crafted peer-to-peer packet through an affected device. A successful exploit could allow the attacker to	2018-04-19	not yet calculated	CVE-2018-0256 CONFIRM

	cause the SESSMGR process on the affected device to restart unexpectedly, which could briefly impact traffic while the SESSMGR process restarts and result in a DoS condition. Cisco Bug IDs: CSCvg88786.			
cisco - staros	A vulnerability in the egress packet processing functionality of the Cisco StarOS operating system for Cisco Aggregation Services Router (ASR) 5700 Series devices and Virtualized Packet Core (VPC) System Software could allow an unauthenticated, remote attacker to cause an interface on the device to cease forwarding packets. The device may need to be manually reloaded to clear this Interface Forwarding Denial of Service condition. The vulnerability is due to the failure to properly check that the length of a packet to transmit does not exceed the maximum supported length of the network interface card (NIC). An attacker could exploit this vulnerability by sending a crafted IP packet or a series of crafted IP fragments through an interface on the targeted device. A successful exploit could allow the attacker to cause the network interface to cease forwarding packets. This vulnerability could be triggered by either IPv4 or IPv6 network traffic. This vulnerability affects the following Cisco products when they are running the StarOS operating system and a virtual interface card is installed on the device: Aggregation Services Router (ASR) 5700 Series, Virtualized Packet Core-Distributed Instance (VPC-DI) System Software, Virtualized Packet Core-Single Instance (VPC-SI) System Software. Cisco Bug IDs: CSCvf32385.	2018-04-19	not yet calculated	CVE-2018-0239 BID SECTRACK CONFIRM

cisco - unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager could allow an authenticated, remote attacker to view sensitive data. The vulnerability is due to insufficient protection of database tables over the web interface. An attacker could exploit this vulnerability by browsing to a specific URL. An exploit could allow the attacker to view configuration parameters. Cisco Bug IDs: CSCvf20218.	2018-04-19	not yet calculated	CVE-2018-0266 BID SECTRACK CONFIRM
cisco - unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager could allow an authenticated, local attacker to view sensitive data that should be restricted. This could include LDAP credentials. The vulnerability is due to insufficient protection of database tables over the web interface. An attacker could exploit this vulnerability by browsing to a specific URL. An exploit could allow the attacker to view sensitive information that should have been restricted. Cisco Bug IDs: CSCvf22116.	2018-04-19	not yet calculated	CVE-2018-0267 BID SECTRACK CONFIRM
cisco - unified_computing_system_director	A vulnerability in the role-based resource checking functionality of the Cisco Unified Computing System (UCS) Director could allow an authenticated, remote attacker to view unauthorized information for any virtual machine in the UCS Director end-user portal and perform any permitted operations on any virtual machine. The permitted operations can be configured for the end user on the virtual machines with either of the following settings: The virtual machine is associated to a Virtual Data Center (VDC) that has an end user self-service policy attached to the VDC. The end user role has VM Management Actions settings configured under User	2018-04-19	not yet calculated	CVE-2018-0238 BID SECTRACK CONFIRM

	Permissions. This is a global configuration, so all the virtual machines visible in the end-user portal will have the VM management actions available. The vulnerability is due to improper user authentication checks. An attacker could exploit this vulnerability by logging in to the UCS Director with a modified username and valid password. A successful exploit could allow the attacker to gain visibility into and perform actions against all virtual machines in the UCS Director end-user portal of the affected system. This vulnerability affects Cisco Unified Computing System (UCS) Director releases 6.0 and 6.5 prior to patch 3 that are in a default configuration. Cisco Bug IDs: CSCvh53501.			
cisco - webex_connect_im	A vulnerability in Cisco WebEx Connect IM could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of an affected system. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected system. An attacker could exploit this vulnerability by convincing a user to follow a malicious link or by intercepting a user request and injecting malicious code into the request. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCvi07812.	2018-04-19	not yet calculated	CVE-2018-0276 BID CONFIRM
cliquemania - cliquemania	CliqueMania loja virtual 14 has SQL Injection via the patch/remote.php id parameter in a recomendar action.	2018-04-21	not yet calculated	CVE-2018-10283 MISC

cloud_foundry_foundation - cloud_foundry_cloud_controller	Cloud Foundry Cloud Controller, capi-release versions prior to 1.0.0 and cf-release versions prior to v237, contain a business logic flaw. An application developer may create an application with a route that conflicts with a platform service route and receive traffic intended for the service.	2018-04-18	not yet calculated	CVE-2016-2169 CONFIRM
cmsmadesimple - cms_made_simple	cmsmadesimple version 2.2.7 contains a Incorrect Access Control vulnerability in the function of send_recovery_email in the line "$url = $config['admin_url'] . '/login.php?recoverme=' . $code;" that can result in Administrator Password Reset Poisoning, specifically a reset URL pointing at an attacker controlled server can be created by using a host header attack.	2018-04-18	not yet calculated	CVE-2018-1000158 MISC
coderium - soundengine_free	Untrusted search path vulnerability in Installer of SoundEngine Free ver.5.21 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2018-04-16	not yet calculated	CVE-2018-0562 JVN CONFIRM
cybozu - cybozu_garoon	Cross-site scripting vulnerability in Cybozu Garoon 3.0.0 to 4.6.1 allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0551 JVN CONFIRM
cybozu - cybozu_garoon	Cybozu Garoon 3.5.0 to 4.6.1 allows remote authenticated attackers to bypass access restriction to view the closed title of "Cabinet" via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0550 JVN CONFIRM
cybozu - cybozu_garoon	Cybozu Garoon 3.0.0 to 4.2.6 allows remote authenticated attackers to bypass access restriction to alter setting data of the Standard database via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0532 JVN CONFIRM
cybozu - cybozu_garoon	Cybozu Garoon 3.0.0 to 4.2.6 allows remote authenticated attackers to bypass access restriction to view or alter an access privilege	2018-04-16	not yet calculated	CVE-2018-0531 JVN

	of a folder and/or notification settings via unspecified vectors.			CONFIRM
cybozu - cybozu_garoon	SQL injection vulnerability in the Cybozu Garoon 3.5.0 to 4.2.6 allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0530 JVN CONFIRM
cybozu - cybozu_garoon	Cross-site scripting vulnerability in Cybozu Garoon 3.0.0 to 4.6.0 allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0549 JVN CONFIRM
cybozu - cybozu_garoon	Cybozu Garoon 3.0.0 to 4.2.6 allows remote authenticated attackers to bypass access restriction to alter setting data of session authentication via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0533 JVN CONFIRM
cybozu - cybozu_garoon	Cybozu Garoon 4.0.0 to 4.6.0 allows remote authenticated attackers to bypass access restriction to view the closed title of "Space" via unspecified vectors.	2018-04-16	not yet calculated	CVE-2018-0548 JVN CONFIRM
d-link - dir-615_t1_devices	D-Link DIR-615 T1 devices allow XSS via the Add User feature.	2018-04-18	not yet calculated	CVE-2018-10110 MISC MISC EXPLOIT-DB
d-link - dir-815_rev.b_devices	D-Link DIR-815 REV. B (with firmware through DIR-815_REVB_FIRMWARE_PATCH_2.07.B01) devices have XSS in the Treturn parameter to /htdocs/webinc/js/bsc_sms_inbox.php.	2018-04-16	not yet calculated	CVE-2018-10108 MISC
d-link - dir-815_rev.b_devices	D-Link DIR-815 REV. B (with firmware through DIR-815_REVB_FIRMWARE_PATCH_2.07.B01) devices have XSS in the RESULT parameter to /htdocs/webinc/js/info.php.	2018-04-16	not yet calculated	CVE-2018-10107 MISC
d-link - dir-	D-Link DIR-815 REV. B (with firmware	2018-04-16	not yet	CVE-2018-

815_rev.b_devices	through DIR-815_REVB_FIRMWARE_PATCH_2.07.B01) devices have permission bypass and information disclosure in /htdocs/web/getcfg.php, as demonstrated by a /getcfg.php?a=%0a_POST_SERVICES%3DDEVICE.ACCOUNT%0aAUTHORIZED_GROUP%3D1 request.		calculated	10106 MISC
dell_emc - vipr_controller	Dell EMC ViPR Controller, versions after 3.0.0.38, contain an information exposure vulnerability in the VRRP. VRRP defaults to an insecure configuration in Linux's keepalived component which sends the cluster password in plaintext through multicast. A malicious user, having access to the vCloud subnet where ViPR is deployed, could potentially sniff the password and use it to take over the cluster's virtual IP and cause a denial of service on that ViPR Controller system.	2018-04-18	not yet calculated	CVE-2018-1240 FULLDISC
digital_guardian - digital_guardian_management_console	Digital Guardian Management Console 7.1.2.0015 allows authenticated remote code execution because of Arbitrary File Upload functionality.	2018-04-20	not yet calculated	CVE-2018-10173 MISC
digital_guardian - digital_guardian_management_console	Digital Guardian Management Console 7.1.2.0015 has an SSRF issue that allows remote attackers to read arbitrary files via file:// URLs, send TCP traffic to intranet hosts, or obtain an NTLM hash. This can occur even if the logged-in user has a read-only role.	2018-04-20	not yet calculated	CVE-2018-10174 MISC
digital_guardian - digital_guardian_management_console	Digital Guardian Management Console 7.1.2.0015 has an XXE issue.	2018-04-20	not yet calculated	CVE-2018-10175 MISC

digital_guardian - digital_guardian_management_console	Digital Guardian Management Console 7.1.2.0015 has a Directory Traversal issue.	2018-04-20	not yet calculated	CVE-2018-10176 MISC
dnn - dnn	The CATALooK.netStore module through 7.2.8 for DNN (formerly DotNetNuke) allows XSS via the /ViewEditGoogleMaps.aspx PortalID or CATSkin parameter, or the /ImageViewer.aspx link or desc parameter.	2018-04-16	not yet calculated	CVE-2018-10138 MISC
domain_trader - domain_trader	XSS exists in Domain Trader 2.5.3 via the recoverlogin.php email_address parameter.	2018-04-16	not yet calculated	CVE-2018-10097 MISC
drupal - drupal	Cross-site scripting (XSS) vulnerability in the Enhanced Image (aka image2) plugin for CKEditor (in versions 4.5.10 through 4.9.1; fixed in 4.9.2), as used in Drupal 8 before 8.4.7 and 8.5.x before 8.5.2 and other products, allows remote attackers to inject arbitrary web script through a crafted IMG element.	2018-04-19	not yet calculated	CVE-2018-9861 CONFIRM CONFIRM

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

GLESEC CYBER SECURITY FLASH REPORT

TLP-GREEN

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