CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Cisco Products

Original Issue Date: 18th May 2017

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Cisco products and they can be exploited by remote attackers to cause execution of arbitrary code, gain knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Cisco Prime Collaboration Provisioning Authentication Bypass Vulnerability **CVE Info:** CVE-2017-6622	A vulnerability has been identified in the web interface for Cisco Prime Collaboration Provisioning and could allow an unauthenticated, remote attacker to bypass authentication and perform command injection with root privileges. The vulnerability is caused due to missing security constraints in certain HTTP request methods, which could allow access to files via the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the targeted application. Successful exploitation could allow the attacker to bypass authentication and perform command injection in Cisco Prime Collaboration Provisioning with root privileges.	Cisco Prime Collaboration Provisioning Software Releases prior to 12.1	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp1
Cisco TelePresence IX5000 Series Directory Traversal Vulnerability	A vulnerability has been identified in the web framework of the Cisco TelePresence IX5000 Series and could allow an unauthenticated,	Cisco TelePresence IX5000 Series devices running software version	Users are advised to apply updates. More information about

CVE Info: CVE-2017-6652	remote attacker to access arbitrary files on an affected device. The vulnerability is caused due to insufficient input validation. This vulnerability could be exploited by using directory traversal techniques to read files within the Cisco TelePresence IX5000 Series filesystem.	8.2.0.	the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-telepresence-ix5000
Cisco Prime Collaboration Provisioning Information Disclosure Vulnerability **CVE Info:** CVE-2017-6621	A vulnerability has been identified in the web interface of Cisco Prime Collaboration Provisioning and this could allow an unauthenticated, remote attacker to access sensitive data. The attacker could make use of this information to conduct additional reconnaissance attacks. The vulnerability is caused due to insufficient protection of sensitive data when responding to an HTTP request on the web interface. An attacker could exploit the vulnerability by sending a crafted HTTP request to the application to access specific system files. An exploit could allow the attacker to obtain sensitive information about the application which could include user credentials.	Cisco Prime Collaboration Provisioning Software Releases 10.6 through 11.5.	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp2
Cisco Policy Suite Privilege Escalation Vulnerability **CVE Info:** CVE-2017-6623	A vulnerability has been reported in a script file that is installed as part of the Cisco Policy Suite (CPS) Software distribution for the CPS appliance and this could allow an authenticated, local attacker to escalate their privilege level to *root*. The vulnerability is caused due to incorrect *sudoers* permissions on the script file. This vulnerability could be	Cisco Policy Suite application is vulnerable when running software versions 10.0.0, 10.1.0, or 11.0.0.	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

	exploited by authenticating to the device and providing crafted user input at the CLI, using this script file to escalate their privilege level and execute commands as *root*. A successful exploit could allow the attacker to acquire *root-level* privileges and take full control of the appliance. The user has to be logged-in to the device with valid credentials for a specific set of users.		20170517-cps
Cisco UCS C-Series Rack Servers TCP Port Denial of Service Vulnerability **CVE Info:** **CVE-2017-6633**	A vulnerability has been identified in the TCP throttling process of Cisco UCS C-Series Rack Servers and this could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on a vulnerable system. The vulnerability is caused due to insufficient rate-limiting protection. An attacker could exploit this vulnerability by sending a high rate of TCP SYN packets to a specific TCP listening port on an affected device. An exploit could allow the attacker to cause a specific TCP listening port to stop accepting new connections, resulting in a DoS condition.	Cisco UCS C-Series Rack Servers.	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucsc
Cisco Unified Communications Manager Cross-Site Scripting Vulnerability **CVE Info:** CVE-2017-6654	A vulnerability has been identified in the web-based management interface of Cisco Unified Communications Manager and this could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of a vulnerable device. The vulnerability is caused due to insufficient validation of user-	Cisco Unified Communications Manager	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucm

	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 IP Phone 8851 Session Initiation Protocol Denial of Service Vulnerability **CVE Info:** CVE-2017-6630	A vulnerability has been identified in the Session Initiation Protocol (SIP) implementation of Cisco IP Phone 8851 and this could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is caused due to an abnormal SIP message. An attacker could exploit this vulnerability by manipulating the CANCEL packet. An exploit could allow the attacker to cause a disruption of service to the phone.	Cisco IP Phone 8851	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-sip
Cisco Remote Expert Manager Multiple Vulnerabilities **CVE Info:** CVE-2017-6647 CVE-2017-6646 CVE-2017-6645 CVE-2017-6644 CVE-2017-6643 CVE-2017-6642 CVE-2017-6641	Multiple vulnerabilities have been identified In Cisco Remote Expert Manager Software and they could allow an unauthenticated, remote attacker to access sensitive information on an affected system.	Default configurations of Cisco Remote Expert Manager Software	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem7
Cisco Prime Collaboration Provisioning Directory Traversal Arbitrary File	A vulnerability has been identified in the web interface of Cisco Prime Collaboration Provisioning Software could allow an authenticated,	Cisco Prime Collaboration Provisioning Software releases	Users are advised to apply updates. More information about the updates is

Deletion Vulnerability **CVE Info:** CVE-2017-6635	remote attacker to delete any file from an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to delete any file from the system.	prior to Release 12.1.	available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp3
Cisco Prime Collaboration Provisioning Directory Traversal Information Disclosure Vulnerability **CVE Info:** **CVE-2017-6636**	A vulnerability has been identified in the web interface of Cisco Prime Collaboration Provisioning Software and this could allow an authenticated, remote attacker to view any file on the vulnerable system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to view any file on the system.	Cisco Prime Collaboration Provisioning Software releases prior to Release 11.1.	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp4
Cisco Nexus 5000 Series Switches Telnet CLI Command	A vulnerability has been identified in the Telnet CLI command of Cisco NX-OS System Software running on	Cisco Nexus 5000 Series Switches in default	Users are advised to apply updates. More information about

Injection Vulnerability **CVE Info:** **CVE-2017-6636**	Cisco Nexus 5000 Series Switches and this could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is caused due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into the Telnet CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside of the user's path.	configurations	the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss1
Cisco Nexus 5000 Series Switches CLI Command Injection Vulnerability **CVE Info:** CVE-2017-6649	A vulnerability has been identified in the CLI of Cisco NX-OS System Software running on Cisco Nexus 5000 Series Switches and this could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is caused due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. Successful exploitation of the vulnerability allowed the attacker to read or write arbitrary files at the user's privilege level outside of the user's path.	Cisco Nexus 5000 Series Switches running in default configurations	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss
Cisco Identity Services Engine GUI Denial of Service Vulnerability **CVE Info:** CVE-2017-6653	A vulnerability has been identified in the TCP throttling process for the GUI of the Cisco Identity Services Engine (ISE) and could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device where the ISE GUI may fail to	Cisco Identity Services Engine (ISE).	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/co

	respond to new or established connection requests. The vulnerability is caused due to insufficient TCP rate limiting protection on the GUI. An attacker could exploit this vulnerability by sending the affected device a high rate of TCP connections to the GUI. An exploit could allow the attacker to cause the GUI to stop responding while the high rate of connections is in progress.		ntent/CiscoSecurityAdvisory/cisco-sa-20170517-ise
Cisco Industrial Ethernet 1000 Series Switches Device Manager Cross-Site Request Forgery Vulnerability **CVE Info:** CVE-2017-6634	A vulnerability has been reported in the Device Manager web interface of Cisco Industrial Ethernet 1000 Series Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected system. The vulnerability is caused 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 and with the privileges of the user.	Cisco Industrial Ethernet 1000 Series Switches	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ie1000csrf
Cisco FirePOWER System Software SSL Logging Denial of Service Vulnerability **CVE Info:** CVE-2017-6632	A vulnerability has been identified in the logging configuration of Secure Sockets Layer (SSL) policies for Cisco FirePOWER System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to high consumption of system resources.	Cisco FirePOWER System Software that is configured to log connections by using SSL policy default actions	Users are advised to apply updates. More information about the updates is available on: https://tools.cisco.com/security/center/co

	The vulnerability is caused due to the logging of certain TCP packets by the affected software. An attacker could exploit this vulnerability by sending a flood of crafted TCP packets to an affected device. A successful exploit could allow the attacker to cause a DoS condition. The success of an exploit is dependent on how an administrator has configured logging for SSL policies for a device.		ntent/CiscoSecurityAdvisory/cisco-sa-20170517-fpwr

Source:

Cisco Security Bulletins

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-fpwr

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ie1000csrf

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ise

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss1

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp4

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp3

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem7

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp1

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-telepresence-ix5000

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-cps

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp2

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucsc

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-sip

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu