National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Cisco Products

Original Issue Date: May 14, 2015

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 and bypass security restrictions on the vulnerable systems. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Command Injection Vulnerability in Multiple Cisco TelePresence Products **CVE Info:** CVE-2015-0713	A vulnerability has been identified in Cisco TelePresence products and could be exploited by remote attackers to inject arbitrary commands with the privileges of the root user. The vulnerability exists due to insufficient input validation. This vulnerability could be exploited by remote attackers by authenticating to the device and submitting crafted input to the affected parameter in a web page.	Cisco TelePresence Advanced Media Gateway Series Cisco TelePresence IP Gateway Series Cisco TelePresence IP VCR Series Cisco TelePresence ISDN Gateway Cisco TelePresence MCU 4200 Series Cisco TelePresence MCU 4500 Series Cisco TelePresence MCU 5300 Series Cisco TelePresence MCU MSE 8420 Cisco TelePresence MCU MSE 8510 Cisco TelePresence Serial Gateway Series Cisco TelePresence Server 7010 Cisco TelePresence Server MSE 8710 Cisco TelePresence Server	Users are advised to apply updates. More information about the updates is available in: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tp

		on Multiparty Media 310 Cisco TelePresence Server on Multiparty Media 320 Cisco TelePresence Server on Virtual Machine	
Multiple Vulnerabilities in Cisco TelePresence TC and TE Software **CVE Info:** CVE-2015-0722 CVE-2014-2174	Multiple vulnerabilities have been identified in Cisco TelePresence TC and TE Software and can be exploited to bypass security measures. The vulnerabilities reported are as follows: • Cisco TelePresence TC and TE Software Authentication Bypass Vulnerability Successful exploitation of this vulnerability could allow an attacker to bypass system authentication and access the device with the privileges of the *root* user. • Cisco TelePresence TC and TE Software Crafted Packets Denial of Service Vulnerability Successful exploitation of this vulnerability could allow an attacker to restart several processes and possibly trigger a reload of the affected system.	Cisco TelePresence MX Series Cisco TelePresence System EX Series Cisco TelePresence Integrator C Series Cisco TelePresence Profiles Series Cisco TelePresence Quick Set Series Cisco TelePresence System T Series Cisco TelePresence VX Clinical Assistant	Users are advised to apply updates. More information about the updates is available in: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tc

Vendor Information
Cisco
www.cisco.com

References

Cisco Security Advisories
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tc
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tp

Security Tracker
http://www.securitytracker.com/id/1032315
http://www.securitytracker.com/id/1032314

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: www.cert-mu.org.mu