National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Cisco Products

Original Issue Date: July 23, 2015

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Cisco products and they can be exploited by remote attackers to bypass security restrictions, take full control of the vulnerable systems and cause a denial of service condition. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
OpenSSL Alternative Chains Certificate Forgery Vulnerability **CVE Info:** CVE-2015-1793	A vulnerability has been identified in OpenSSL and could be exploited by remote attackers to bypass security checks. The vulnerability is caused due to an error in the implementation of the logic for finding an alternative certificate chain if the first attempt to build such chain fails. This vulnerability can cause an unauthenticated remote attacker to submit a crafted certificate chain to an affected device during SSL, TLS, or DTLS authentication. Successful exploitation could allow the attacker to cause certain checks on untrusted certificates to be bypassed, enabling the attacker to forge "trusted" certificates that could be used to conduct man-in-the-middle attacks.	Cisco WebEx Node for MCS Cisco Agent for OpenFlow Cisco Jabber Software Development Kit Cisco Jabber for Android WebEx Recording Playback Client Cisco ASA CX and Cisco Prime Security Manager Cisco Virtual Security Gateway for Microsoft Hyper-V List of other affected software is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150710-openssl	Users are advised to apply updates. More information about the updates is available in: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150710-openssl

Cisco Application Policy Infrastructure Controller Access Control Vulnerability **CVE Info:** CVE-2015-4235	A vulnerability has been identified in the cluster management configuration of the Cisco Application Policy Infrastructure Controller (APIC) and the Cisco Nexus 9000 Series ACI Mode Switch could allow an authenticated, remote attacker to access the APIC as the root user. The vulnerability is caused due to improper implementation of access controls in the APIC filesystem. This vulnerability can be exploited by remote attackers to access the cluster management configuration of the APIC. Successful exploitation of the vulnerability can allow the attacker to gain access to the APIC as the root user and perform root-level commands.	Application Policy Infrastructure Controllers running software versions prior to 1.1(1j), 1.0(3o) and 1.0(4o) Cisco Nexus 9000 Series ACI Mode Switches running software versions prior to Release 11.1(1j) and 11.0(4o)	Currently, there are no workarounds for this vulnerability.
Cisco IOS Software TFTP Server Denial of Service Vulnerability **CVE Info:** CVE-2015-0681	A vulnerability has been identified in TFTP server functionality of Cisco IOS and Cisco IOS XE Software. This vulnerability is caused due to incorrect management of memory when handling TFTP requests. Successful exploitation of the vulnerability can allow remote attackers to make a number of TFTP requests to the affected device. Successful exploitation of the vulnerability can allow the attacker to cause the device to reload or hang.	Cisco IOS and Cisco IOS XE Software devices that are running an affected version of software are vulnerable.	Users are advised to completely disable the TFTP server. More information is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-tftp
Cisco Unified MeetingPlace Unauthorized Password Change Vulnerability **CVE Info:** CVE-2015-4262	A vulnerability has been identified in password change functionality in the Cisco Unified MeetingPlace Web Conferencing application application. The vulnerability is due to the following: • Users are not required to enter the previous password during a password change request. • HTTP session functionality does not validate the session ID in the HTTP request for the password change request. This vulnerability can be exploited via a crafted HTTP request and change arbitrary user passwords to gain access to the application. Successful exploitation of the vulnerability can allow remote attackers to use the reset credentials to gain full control of the application. This vulnerability can be exploited	Cisco Unified MeetingPlace Web Conferencing versions prior to 8.6	Currently, there are no workaround for this vulnerability.

	by remote attackers to change passwords of arbitrary users.		

Vendor Information
Cisco
www.cisco.com

References

Cisco Security Bulletins
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-mp
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-tftp
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-apic
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-tftp

Security Tracker
http://www.securitytracker.com/id/1033024
http://www.securitytracker.com/id/1033023
http://www.securitytracker.com/id/1033025

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