National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Cisco Products

Original Issue Date: May 2014

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 on vulnerable systems, obtain elevated privileges, conduct cross-site request forgery, gain knowledge of sensitive information and inject SQL commands. Cisco has released an update that addresses all the vulnerabilities. The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Cisco NX-OS Multiple Vulnerabilities **CVE Info:** CVE-2014-3261 CVE-2014-2201 CVE-2014-2200 CVE-2013-1191	• Cisco NX-OS	Multiple vulnerabilities have been identified in Cisco NX-OS and they can be exploited by remote attackers cause execution of arbitrary code and gain elevated privileges on affected systems. The vulnerabilities reported are as follows: • On systems with multiple virtual device contexts (VDC), a remote authenticated user on the SSH management interface can exploit an SSH key file privilege escalation flaw to gain the privileges of an administrator in a different VDC. • Another vulnerability exists	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

		that can allow a remote user to send a large amount of specially crafted data to trigger a null pointer dereference in the Message Transfer Service (MTS) and cause a kernel panic. • A vulnerability occurs that can allow a remote SMTP server to return specially crafted data to trigger a buffer overflow in the Smart Call Home feature to execute arbitrary code with elevated privileges on the target device. • On systems with multiple virtual device contexts (VDC), a remote authenticated user on the SSH management interface can exploit an SSH privilege escalation flaw to gain the privileges of an administrator in a different VDC.	
Cisco Security Manager Input Validation Flaw Permits Cross-Site Request Forgery Attacks **CVE Info:** **CVE-2014-3267**	• Cisco Security Manager	A vulnerability has been identified in Cisco Security Manager and it can be exploited by remote attackers to conduct cross-site request forgery attacks. The vulnerability occurs the web framework does not properly validate user-supplied input. Successful exploitation of the vulnerability can allow a remote attacker to create a specially crafted URL that when loaded by the user will take actions on the Cisco Security Manager interface acting as the target user.	Users are advised to apply updates. More information is available on: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3267

Cisco TelePresence Does Not Always Encrypt Directory Information Transfers **CVE Info:** **CVE-2014-3274**	• Cisco TelePresence	A vulnerability has been identified in Cisco TelePresence. This vulnerability occurs because the system does not enforce HTTPS when transferring directory information between the Cisco TelePresence System (CTS) and the Cisco Unified Communications Manager (Cisco UCM). This vulnerability can allow a remote user monitoring the network can block an HTTPS connection and then monitor the directory information sent via an HTTP connection. Successful exploitation of the vulnerability can allow gaining sensitive information.	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3274
Cisco Identity Services Engine Vulnerability **CVE Info:** **CVE-2014-3275**	• Cisco Identity Services Engine	A vulnerability has been identified in Cisco Identity Services Engine and it can be exploited by remote attackers to inject SQL commands. The vulnerability occurs because the software does not properly validate user-supplied input. Successful exploitation of the vulnerability can allow a remote attacker to supply a specially crafted parameter value to execute SQL commands on the underlying database.	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3275
Cisco Tidal Enterprise Scheduler Agent **CVE Info:** **CVE-2014-3272**	• Cisco Tidal Enterprise Scheduler	A vulnerability has been reported in Cisco Tidal Enterprise Scheduler. This vulnerability can allow a local user to obtain elevated privileges on the target system. Successful exploitation of the vulnerability can allow remote attackers to cause execution of	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3272

		arbitrary code on the vulnerable system with root privileges.	

Vendor Information

Cisco

www.cisco.com

References

Cisco Security Notice

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3272

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3275

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3274

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3275

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3267

Security Tracker

http://www.securitytracker.com/id/1030271

http://www.securitytracker.com/id/1030268

http://www.securitytracker.com/id/1030272

http://www.securitytracker.com/id/1030273

http://www.securitytracker.com/id/1030275

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-mu.gov.mu.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: www.cert-mu.org.mu