National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

TA-2015-10

Multiple Vulnerabilities in Cisco Products

Original Issue Date: 25 March 2015

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Cisco Products and they can be exploited by remote attackers to cause denial of service condition and gain knowledge of sensitive information Cisco has released an update that addresses all the vulnerabilities. The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerability **CVE Info:** **CVE-2015-0646**	• Cisco devices that are running affected Cisco IOS Software or Cisco IOS XE Software	A vulnerability has been identified in the TCP input module of Cisco IOS and Cisco IOS XE Software and can be exploited by remote attackers to cause a memory leak and eventual reload of the affected device. The vulnerability is due to improper handling of certain crafted packet sequences used in establishing a TCP three-way handshake. An attacker could exploit this vulnerability by sending a crafted sequence of TCP packets while establishing a three-way handshake. Successful exploitation could allow the attacker to cause a memory leak and eventual reload of the affected	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

		device.	
Multiple Vulnerabilities in Cisco IOS Software and IOS XE Software Autonomic Networking Infrastructure **CVE Info:** **CVE-2015-0635** **CVE-2015-0636** **CVE-2015-0637**	• Cisco ASR 901, 901S, and 903 Series Aggregation Services Routers • Cisco ME 3600, 3600X, and 3800X Series Ethernet Access Switches	Multiple vulnerabilities have been identified in the Autonomic Networking Infrastructure (ANI) feature of Cisco IOS Software and IOS XE Software and could allow remote attackers to cause a denial of service (DoS) condition or gain limited command and control of the device. The following vulnerabilities have been identified: • Autonomic Networking Registration Authority Spoofing Vulnerability • Autonomic Networking Infrastructure Spoofed Autonomic Networking Messages Denial of Service Vulnerability • Autonomic Networking Infrastructure Device Reload Denial of Service Vulnerability	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ani
Cisco IOS Software and IOS XE Software Internet Key Exchange Version 2 Denial of Service Vulnerabilities **CVE Info:** **CVE-2015-0642** **CVE-2015-0643**	• Devices running Cisco IOS Software or Cisco IOS XE Software are vulnerable when IKEv1 or ISAKMP is enabled	Multiple vulnerabilities have been reported in devices running Cisco IOS Software or IOS XE Software and could be exploited by remote attackers to cause a denial of service (DoS) condition. The vulnerabilities exist because an affected device processes certain malformed IKEv2 packets. This could be exploited by remote attackers to send malformed IKEv2 packets to an affected device to be processed. Successful exploitation could allow the	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ikev2

		attacker to cause a reload of the affected device or excessive consumption of resources that would lead to a DoS condition.	
Cisco IOS Software and IOS XE Software mDNS Gateway Denial of Service Vulnerability **CVE Info:** **CVE-2015-0650**	• Cisco devices that are running affected Cisco IOS Software or Cisco IOS XE Software are vulnerable	A vulnerability has been identified in the multicast DNS (mDNS) gateway function of Cisco IOS Software and Cisco IOS XE Software and could allow remote attackers to reload the vulnerable device. The vulnerability is caused due to improper validation of mDNS packets. This vulnerability could be exploited by sending malformed IP version 4 (IPv4) or IP version 6 (IPv6) packets on UDP port 5353. Successful exploitation could allow an attacker to cause a denial of service (DoS) condition.	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-mdns
Multiple Vulnerabilities in Cisco IOS Software Common Industrial Protocol **CVE Info:** **CVE-2015-0649** **CVE-2015-0648** **CVE-2015-0647**	• Cisco IOS	Multiple vulnerabilities have been identified in the Cisco IOS Software implementation of the Common Industrial Protocol (CIP) feature and can be exploited by remote attackers to cause a denial of service condition. The following vulnerabilities have been reported: • Cisco IOS Software UDP CIP Denial of Service Vulnerability • Cisco IOS Software TCP CIP Packet Memory Leak Vulnerability • Cisco IOS Software TCP CIP Denial of Service Vulnerability	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-cip

		Successful exploitation of any of these vulnerabilities could allow a remote attacker to cause a reload of the forwarding plane, resulting in an interruption of services on an affected device. Repeated exploitation could result in a sustained DoS condition.	
Multiple Vulnerabilities in Cisco IOS XE Software for Cisco ASR 1000 Series, Cisco ISR 4400 Series, and Cisco Cloud Services 1000v Series Routers **CVE Info:** **CVE-2015-0639** **CVE-2015-0645** **CVE-2015-0641** **CVE-2015-0644**	• Cisco IOS XE Software for Cisco ASR 1000 Series Routers • Cisco 4400 Series ISRs • Cisco CSR 1000v Series	Multiple vulnerabilities have been identified in Cisco IOS XE Software for Cisco ASR 1000 Series Aggregation Services Routers (ASR), Cisco 4400 Series Integrated Services Routers (ISR), and Cisco Cloud Services Routers (CSR) 1000v Series. The vulnerabilities reported are as follows: • Cisco IOS XE Software Fragmented Packet Denial of Service Vulnerability • Cisco IOS XE Software Crafted TCP Packet Remote Code Execution Vulnerability • Cisco IOS XE Software Crafted IPv6 Packet Denial of Service Vulnerability • Cisco IOS XE Software Layer 4 Redirect Crafted Packet Denial of Service Vulnerability • Cisco IOS XE Software Common Flow Table Crafted Packet Denial of Service Vulnerability Successful exploitation of any of these vulnerabilities could allow	Users are advised to apply updates. More information about the updates is available on: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-iosxe

		remote attacker to trigger a reload of the forwarding plane, causing an interruption of services. Repeated exploitation could result in a sustained denial of service (DoS) condition.	

Vendor Information

Cisco

www.cisco.com

References

Cisco Security Notice

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ani

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-cip

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ikev2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-mdns

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-iosxe

Security Tracker

http://www.securitytracker.com/id/1031982

http://www.securitytracker.com/id/1031984

http://www.securitytracker.com/id/1031981

http://www.securitytracker.com/id/1031980

http://www.securitytracker.com/id/1031979

http://www.securitytracker.com/id/1031978

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