National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

CERT-MU

Targeted Security Alert

Cisco IOS XR Software IPv6 Malformed Packet Denial of Service Vulnerability

Original Issue Date: February 2015

Severity Rating: High

Potential Security Impact: Reload of the affected line card

Software Affected:

Cisco Network Convergence System 6000 (NCS 6000) and Cisco Carrier Routing System X (CRS-X) running an affected version of Cisco IOS XR Software are affected.

Overview:

A critical vulnerability has been identified in the parsing of malformed IP version 6 (IPv6) packets in Cisco IOS XR software.

Description:

A vulnerability has been identified in the parsing of malformed IPv6 packets in Cisco IOS XR Software for Cisco NCS 6000 and Cisco CRS-X. This vulnerability can allow a remote attacker to cause a reload of a line card that is processing traffic. The vulnerability exists because malformed IPv6 packets carrying extension headers are not processed properly. An attacker can exploit this vulnerability by sending a malformed IPv6 packet, carrying extension headers, through an affected Cisco IOS XR device line card. Successful exploitation of this vulnerability can allow attackers to cause a reload of the line card on the vulnerable systems.

Solution

Cisco has released a workaround that address the vulnerability. For the deployment, please refer to the link below:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150220-ipv6

Vendor Information

Cisco
www.cisco.com

References

Cisco Security Advisory
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150220-ipv6

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