CERT-MU AD-2016-07

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 30 September 2016

Severity Rating: High

Overview:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, cause target service to restart, obtain potentially sensitive information, perform SQL injection, obtain elevated privileges, cause target system to reload, gain full control of the target system and conduct cross-site request forgery (CSRF) attack on the target system. Cisco has issued updates and workaround(s) to address these vulnerabilities.

Description:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, cause target service to restart, obtain potentially sensitive information, perform SQL injection, obtain elevated privileges, cause target system to reload, obtain complete control over an affected system and conduct cross-site request forgery (CSRF) attack on the target system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in Cisco IOS XR. This vulnerability exists because of a memory error in OSPF. This vulnerability could be exploited by remote attackers by sending a specially crafted Open Shortest Path First (OSPF) Link State Advertisement (LSA) update to the target device. Successful exploitation of this vulnerability could allow an attacker to trigger a memory error and cause the OSPF process to restart.

- Multiple vulnerabilities have been identified in Cisco IOS and IOS XE. These vulnerabilities could allow remote attackers to cause the target system or service

to reload, view portions of process memory, and corrupt information in the local DNS cache of the target system.

- The following are affected:
  - IPv4 Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message processing from a configured MSDP peer.
  - IPv6 Protocol Independent Multicast (PIM) register message packets received by a PIM rendezvous point (RP).
  - IPv4 fragment reassembly processing for packets sent to the target device.
  - Authentication, Authorization, and Accounting (AAA) authentication error log message processing.
  - H.323 message processing
  - The processing of fragmented Internet Key Exchange version 1 (IKEv1) UDP packets directed to the target system via IPv4 or IPv6.
  - The processing of Common Industrial Protocol (CIP) message requests.
  - The processing of specially crafted ICMP packets that require Network Address Translation (NAT).
  - The processing of Smart Install packets received on TCP port 4786 on a Cisco Catalyst switch.

Successful exploitation of these vulnerabilities could allow remote to cause the target system or service to reload, view portions of process memory, and corrupt information in the local DNS cache of the target system.

- A vulnerability has been identified in Cisco Content Security Management Appliance, Cisco Web Security Appliance and Cisco Email Security Appliance. This vulnerability exists because of lack of throttling of FTP connections. This vulnerability could be exploited by remote attackers by sending a flood of FTP traffic to the target service. Successful exploitation of this vulnerability could allow an attacker to cause denial of service conditions.
- A vulnerability has been identified in Cisco FireSIGHT. This vulnerability exists because of insufficient CSRF protections by an affected device. This vulnerability could be exploited by remote attackers by creating a specially

crafted HTML page or URL that, when loaded by the target authenticated user, will take actions on the target interface acting as the target user.

- A vulnerability has been identified in the web framework of the Cisco Firepower Management Center. This vulnerability exists because of improper authorization checks for authenticated users of the system. This vulnerability could be exploited by remote attackers by sending specially crafted data to exploit an authorization check flaw in the web framework. Successful exploitation of this vulnerability could allow an attacker to obtain information on the target system that is outside of their assigned role.

- A vulnerability has been identified in Cisco IronPort AsyncOS for Cisco Email Security Appliances (ESA). This vulnerability exists because of the presence of a Cisco internal testing and debugging interface (intended for use during product manufacturing only) on customer-available software releases. This vulnerability could be exploited by remote attackers by connecting to this testing and debugging interface. Successful exploitation of this vulnerability could allow an attacker to obtain complete control of an affected device with root-level privileges.

Impact of the attack(s)

Remote attackers can:

- cause system restart
- cause denial of service conditions
- conduct cross-site request forgery (CSRF) attacks
- gain full control of the target system
- obtain potentially sensitive information
- perform SQL injection,
- obtain elevated privileges
- cause target system to reload

Affected System:

- Cisco Firepower Management Center running on Cisco FireSIGHT System Software.
- Cisco Firepower Management Center and FireSIGHT System Software.
- Cisco Email Security Appliance (ESA) 9.1.2-023, 9.1.2-028, 9.1.2-036, 9.7.2-046, 9.7.2-047, 9.7-2-054, 10.0.0-124, 10.0.0-125
- Cisco Content Security Management Appliance (SMA)
- Cisco Web Security Appliance (WSA)
- Cisco IOS Software or Cisco IOS XE Software:

    - Cisco cBR Series Converged Broadband Routers
    - Cisco uBR7200 Series Universal Broadband Routers
    - Cisco uBR7225VXR Universal Broadband Routers
    - Cisco uBR10000 Series Universal Broadband Routers
- Cisco IOS XR Software

CVE Information:
CVE-2016-6421
CVE-2016-6378
CVE-2016-6379
CVE-2016-6380
CVE-2016-6381
CVE-2016-6416
CVE-2016-6417
CVE-2016-6420
CVE-2016-6406

More CVE information available on http://securitytracker.com/id/1036914

Solution
Users are advised to apply updates.
More information about the updates is available on:

References:

Security Tracker

http://securitytracker.com/id/1036909

http://securitytracker.com/id/1036914

http://securitytracker.com/id/1036915

http://securitytracker.com/id/1036916

http://securitytracker.com/id/1036917

http://securitytracker.com/id/1036918

http://securitytracker.com/id/1036919

Cisco

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ospf
https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56513
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ipdr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-msdp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-smi
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-aaados
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-frag
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-cip
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-dns
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-esp-nat
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-aos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-fmc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-fmc1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-vds
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa

Cisco Security Advisories and Alerts
https://tools.cisco.com/security/center/publicationListing.x?product=Cisco#~Vulnerabilities

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, 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: http://cert-mu.org.mu