CERT-MU AD-2016-10

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 20 October 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, conduct cross-site request forgery, execute arbitrary request, bypass Snort detection, retrieve memory from server, cause the target system to restart and obtain full control of the 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, conduct cross-site request forgery, execute arbitrary request, can bypass Snort detection, retrieve memory from server, cause the target system to restart and obtain full control of the system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in Cisco IOS and Cisco IOS XE.This vulnerability allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition due to low memory. The vulnerability exists due to the handling of out-of-order, or otherwise invalid, TCP packets on a remote connection to an affected device. An attacker could exploit this vulnerability by connecting to the device and then sending crafted TCP packets that are out of order or have invalid flags. On successful exploiation, the attacker can cause the device to report low-memory warnings, which could in turn cause a partial DoS condition.

- A vulnerability has been identified in Cisco ASA. This vulnerability could allow an unauthenticated, remote attacker to cause the affected system to reload. The vulnerability exists due to improper handling of crafted packets during the enrollment operation. An attacker can send a specially crafted enrollment request to the affected system. On successful exploitation, the attacker can cause the target system to reload.

- A vulnerability has been identified in Cisco Meeting Server. This vulnerability could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a Web Bridge user. The vulnerability exists due to insufficient CSRF protections. Moreover, an attacker could exploit this vulnerability by convincing the user of the affected system to follow a malicious link or visit an attacker-controlled website. On successful exploitation an attacker will be able to submit arbitrary requests to the affected device via the Web Bridge with the privileges of the user.

- Vulnerability has been identified in Web Bridge for Cisco Meeting Server. This vulnerability could allow an unauthenticated, remote attacker to retrieve memory from a connected server. The vulnerability exists due to missing bounds checks in the Web Bridge functionality. An attacker could exploit this vulnerability by sending a crafted packet to the affected server. A successful exploitation could allow the attacker to disclose a portion of memory from the server for every packet. The disclosed portions of memory could contain sensitive information such as private keys or passwords.

- A vulnerability has been identified in the detection engine reassembly of HTTP packets for Cisco Firepower System Software. This vulnerability could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to the Snort process unexpectedly restarting. The vulnerability exists due to improper handling of an HTTP packet stream. An attacker could send a crafted HTTP packet stream to the detection engine on the targeted device. A successful exploitation a remote user can cause the target service to restart and can bypass Snort detection.

- A vulnerability has been the Identity Firewall feature of Cisco ASA. This vulnerability could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability exists due to a buffer overflow in the affected code area. An attacker could send a crafted NetBIOS packet in response to a NetBIOS probe sent by the ASA software. On successful exploitation an attacker will be able to execute arbitrary code and

obtain full control of the system or cause a reload of the affected system.

Impact of the attack(s)

Remote attackers can:

- Cause denial of service conditions
- Conduct cross-site request forgery
- Execute arbitrary request
- Bypass snort detection
- retrieve memory from server
- cause the target system to restart
- obtain full control of the system

Affected System:

- Cisco IOS and Cisco IOS XE
- Cisco Meeting Server
- Firepower 4100 &9300 Series Security Appliances
- FirePOWER 7000& 8000 Series Appliances
- Sourcefire 3D System Appliances
- Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco Catalyst 6500 Series/7600 Series ASA Services Module
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco ISA 3000 Industrial Security Appliance

CVE Information:

CVE-2015-6289
CVE-2016-6431
CVE-2016-6432
CVE-2016-6439
CVE-2016-6444
CVE-2014-6446

Solution

Users are advised to apply updates.

More information about the updates is available on:

References:

Security Tracker

http://securitytracker.com/id/1037059
http://securitytracker.com/id/1037060
http://securitytracker.com/id/1037061

Cisco

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-isr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-ca
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms1
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-fpsnort
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-idfw

Cisco Security Advisories and Alerts

https://tools.cisco.com/security/center/publicationListing.x

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