CERT-MU Advisory

CERT-MU

CERT-MU AD-2016-03

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 18 August 2016

Severity Rating: High

Overview:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote / local attackers to gain elevated privileges, execute arbitrary commands, cause a system reload and cause denial of service condition on the target system. Cisco has issued updates and workaround(s) to addresses these vulnerabilities.

Description:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote / local attackers to gain elevated privileges, execute arbitrary commands, cause a system reload and cause denial of service condition on the target system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in Cisco Aironet. This vulnerability exists because of improper sanitization of user input for certain commands at the command line-interface (CLI). This vulnerability could be exploited by local attackers by supplying specially crafted CLI parameters to trigger an input validation flaw and execute arbitrary commands on the target system with root privileges.

- A vulnerability has been identified in Cisco Aironet, 802.11 wireless LAN protocol for Cisco Access Point (AP) platforms. This vulnerability exists because of rate limiting of 802.11 traffic. This vulnerability could be exploited by remote attackers

by sending specially crafted 802.11 data to the target device in order to trigger a rate limiting error and thus cause a device reload.

- A vulnerability has been identified in Cisco Adaptive Security Appliance (ASA). This vulnerability exists because of a buffer overflow in the affected code area. This vulnerability could be exploited by remote attackers provided they are aware of the Simple Network Management Protocol (SNMP) community string by sending specially crafted SNMP packets to the affected system in order to cause execution of arbitrary code, obtain full control and cause the system to reload.

- A vulnerability has been identified in Cisco Adaptive Security Appliance (ASA). This vulnerability could allow a local unauthenticated attacker to supply specially crafted commands to trigger a flaw in the command-line interface (CLI) parser and deny service or execute arbitrary commands on the target system with root privileges.

- A vulnerability has been identified in Cisco ASA 5500-X Series with FirePOWER Services. This vulnerability exists because of a lack of authorization checking. This vulnerability could be exploited by remote attackers by sending specially crafted HTTP requests to the affected device. Successful exploitation of this vulnerability could allow remote attackers to execute system commands with root-level privileges.

- A vulnerability has been identified in Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM). This vulnerability exists because of improper sanitization of input during the Grapevine update process. This vulnerability could be exploited by remote attackers by sending specially crafted parameter value to trigger an input validation flaw in the Grapevine update process to execute arbitrary operating system commands on the target system.

- A vulnerability has been identified in Cisco 8800 Series IP Phones. This vulnerability exists because of insufficient validation of user-supplied input by the affected software. This vulnerability could be exploited by remote attackers by sending specially crafted malicious HTTP request to the target device to trigger a memory corruption error thus causing denial of service (DoS) conditions.

Impact of the attack(s)

A remote / local attacker can:

- cause memory corruption that results in a DoS condition,
- cause the target system to reload,
- obtain root privileges on the target system,
- execute arbitrary commands on the target system with root privileges,
- execute arbitrary operating system commands on the target system with root privileges.

Affected System:

- Cisco Aironet 1800, 2800, and 3800 AP platforms versions prior to 8.2.110.0, 8.2.121.0, or 8.3.102.0.
- Cisco Aironet 1800, 2800, and 3800 AP platforms versions prior to 8.2.121.0 or 8.3.102.0.
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module, Cisco PIX Firewalls
- Cisco Firewall Services Module (FWSM)
- Cisco ASA 5500 , 5500-X Series prior to 8.4(1)
- Cisco PIX Firewalls
- Cisco Firepower Management Center and Cisco ASA 5500-X Series with FirePOWER Services versions 5.4.0, 5.3.1, 5.3.0.4, 5.2.0, and 4.10.3.9.
- Cisco APIC-EM 1.0.
- Cisco IP Phone 8800 Series version 11.0(1).

CVE Information:

CVE-2016-6362
CVE-2016-6363
CVE-2016-6366
CVE-2016-6367
CVE-2016-1457
CVE-2016-1365
CVE-2016-1479

Solution
Users are advised to apply updates.
More information about the updates is available on:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-fmc

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-apic

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ipp

References:
Security Tracker
http://securitytracker.com/id/1036644

http://securitytracker.com/id/1036645

http://securitytracker.com/id/1036637

http://securitytracker.com/id/1036636

http://securitytracker.com/id/1036642

http://securitytracker.com/id/1036634

http://securitytracker.com/id/1036646

Cisco
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-fmc

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-apic

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ipp

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