**CERT-MU AD-2016-05**

# MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

**Original Issue Date:** 01 September 2016

**Severity Rating:** High

**Overview:**

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to execute arbitrary commands, cause denial of service condition, allow unauthorised access, conduct cross-site scripting (XSS) attack, travers directories 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 execute arbitrary commands, cause denial of service condition, allow unauthorised access, conduct cross-site scripting (XSS) attack, travers directories and conduct cross-site request forgery (CSRF) attack on the target system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in the web interface of Cisco Hosted Collaboration Mediation Fulfillment. This vulnerability exists because of improper input verification and sanitization of the user input directory path. This vulnerability could be exploited by remote attackers by sending specially crafted HTTP request to the affected device and allow the attacker to read arbitrary files on the system that should be restricted.

- A vulnerability has been identified in the web interface of Cisco Hosted Collaboration Mediation Fulfillment. This vulnerability exists because of improper input validation of the HTTP URL format. This vulnerability could be exploited by

sending specially crafted HTTP to the affected application and allow the attacker to write out an arbitrary file.

- A vulnerability has been identified in the Cisco WebEx Meetings Player. This vulnerability exists because of lack of proper handling of user-supplied files. This vulnerability could be exploited by an attacker by persuading a user to open a malicious file by using the affected software and this could allow the attacker to execute arbitrary code on the system with the privileges of the user.

- A vulnerability has been identified in the HTTP framework of Cisco Small Business SPA300 Series IP Phones, Cisco Small Business SPA500 Series IP Phones, and Cisco SPA51x IP Phones. This vulnerability exists because of incorrect handling of malformed HTTP traffic. This vulnerability could be exploited by an attacker by sending specially crafted HTTP requests to an affected device and continuously deny service by sending crafted HTTP requests to a phone, thus resulting in a denial of service condition.

- A vulnerability has been identified in the web-based management interface of Cisco Small Business 220 Series Smart Plus (Sx220) Switches. This vulnerability exists because of insufficient CSRF protections for the web-based management interface of an affected device. This vulnerability could be exploited by an attacker by persuading a user of the interface to click on a specially crafted link thus allowing the attacker to perform arbitrary actions on a targeted device via a web browser and with the privileges of the user.

- A vulnerability has been identified in the web-based management interface of Cisco Small Business 220 Series Smart Plus (Sx220) Switches. This vulnerability exists because of inadequate validation of user-supplied input by the web-based management interface of an affected device. This vulnerability could be exploited by an attacker by persuading a user of the interface to click on a specially crafted link thus allowing the execution of arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.

- A vulnerability has been identified in the implementation of Simple Network Management Protocol (SNMP) functionality in Cisco Small Business 220 Series Smart Plus (Sx220) Switches. This vulnerability exists because of the presence of a default SNMP community string that is added during device installation and cannot be deleted. This vulnerability could be exploited by an attacker by using the default SNMP community string to access SNMP objects on an affected

device and this could allow an attacker to view and modify SNMP objects on a targeted device.

- A vulnerability has been identified in the application programming interface (API) for the Platform and Applications Manager (PAM) for the Cisco Virtual Media Packager (VMP). This vulnerability exists because of improper authentication controls. This vulnerability could be exploited by an attacker by accessing the PAM API without authentication.

- A vulnerability has been identified in the Cisco WebEx Meetings Player. This vulnerability exists because of inadequate validation of user-supplied files. This vulnerability could be exploited by an attacker by persuading a user to open a malicious file by using the affected software and cause WebEx Meetings Player to crash, thus causing denial of service condition on the target system.

- A vulnerability has been identified in the traffic stream metrics (TSM) implemented with the Inter-Access Point Protocol (IAPP) of the Cisco Wireless LAN Controller (WLC). This vulnerability occurs when an SNMP request for TSM information is received. This vulnerability could be exploited by an attacker by sending specially crafted IAPP packets followed by an SNMP request for TSM information to the targeted device and cause a DoS condition when the WLC unexpectedly restarts.

- A vulnerability has been identified in the Cisco Adaptive Wireless Intrusion Prevention System (wIPS) implementation in the Cisco Wireless LAN Controller (WLC). This vulnerability exists because of improper input validation of wIPS protocol packets. This vulnerability could be exploited by an attacker by sending a malformed wIPS packet to the affected device and thus causing a DoS condition when the wIPS process on the WLC unexpectedly restarts.

**Impact of the attack(s)**

Remote attackers can:

- cause system restart
- travers directories and obtain files on the target system
- travers directories and write files on the target system
- cause denial of service conditions
- cause the target application to crash
- conduct cross-site scripting attacks
- access and modify data

- execute arbitrary commands
- conduct cross-site request forgery attacks
- cause the target management interface to stop responding
- gain full control of the target system

**Affected System:**

- Cisco WebEx Meetings Player version T29.10 for WRF files.
- Cisco Wireless LAN Controller prior to versions 8.0.140.0, 8.2.121.0, and 8.3.102.0.
- Cisco Virtual Media Packager (VMP) using Media Origination System Suite Software versions 2.6 and prior.
- Cisco Small Business 220 Series Smart Plus (Sx220) Switches versions 1.0.0.17, 1.0.0.18, or 1.0.0.19.
- Cisco Small Business IP Phones version 7.5.7(6) or prior , SPA300 Series IP Phones, SPA500 Series IP Phones, SPA51x IP Phones.
- Cisco WebEx Meetings Player version T29.10.
- Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) versions 10.6(3) and prior.

**CVE Information:**

CVE-2016-1415

CVE-2016-1464

CVE-2016-1469

CVE-2016-1473

CVE-2016-6376

CVE-2016-6375

CVE-2016-6377

CVE-2016-1472

CVE-2016-1471

CVE-2016-1470

CVE-2016-6371

CVE-2016-6370

**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-20160831-hcm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcmf

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-spa

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-vmp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-webex

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-2

**References:**

**Security Tracker**
http://securitytracker.com/id/1036713

http://securitytracker.com/id/1036712

http://securitytracker.com/id/1036717

http://securitytracker.com/id/1036711

http://securitytracker.com/id/1036718

http://securitytracker.com/id/1036719

http://securitytracker.com/id/1036721

http://securitytracker.com/id/1036722

http://securitytracker.com/id/1036723

http://securitytracker.com/id/1036724

**Cisco**

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcm

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcmf

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-spa

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps3

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-vmp

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-webex

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-2

**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