Security Update:Cisco Released 2 Critical, 2 High and 10 Medium Security Updates for Various Cisco Products

Cisco Released 2 Critical, 2 High and 10 Medium Security Updates for Various Cisco Products

Status Type

Security Update

Private

Public

Date and Time

Monday, August 22, 2016 - 10:03

Reason

Security Update

Impact

Cisco Product Users

WHAT HAPPENED?
Cisco released security updates to address vulnerabilities in multiple products.

Advanced Users: For a complete description of the vulnerabilities visit:

CRITICAL:

- Cisco Firepower Management Center Privilege (Escalation Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [1]
- Cisco Firepower Management Center Remote Command (Execution Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [2]

HIGH:

- Cisco Application Policy Infrastructure Controller Enterprise Module (Remote Code Execution Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [3]
- Cisco Adaptive Security Appliance (SNMP Remote Code Execution Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [4]

MEDIUM:

- Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms (AMPDU Denial of Service Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [5]
- Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms (CLI Privilege Escalation Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [6]
- Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms (802.11 Protocol Denial of Service Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [7]
- Cisco Adaptive Security Appliance (CLI Remote Code Execution Vulnerability (link is external)) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [8]
- Cisco Firepower Management Center (Cross-Site Scripting Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [9]
- Cisco IP Phone 8800 Series (Denial of Service Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [10]
- Cisco Identity Services Engine Admin Dashboard Page (Cross-Site Scripting Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [11]
- Cisco Smart Call Home Transport Gateway (Cross-Site Scripting Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [12]
- Cisco Unified Communications Manager (Information Disclosure Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [13]
- Cisco WebEx Meetings Server (Information Disclosure Vulnerability) at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis... [14]

AFFECTED VERSIONS:
Users and administrators are encouraged to review the Cisco Security Advisories (listed above).

WHAT'S THE PROBLEM?
Exploitation of one of these vulnerabilities could allow an attacker to take control of an affected system and/or view confidential data.

WHAT DO I NEED TO DO?
Users and administrators are encouraged to review the Cisco Security Advisories listed in the "WHAT HAPPENED?? section and apply the necessary updates:

RELATED LINKS

- **IT Security** at http://it.ucsf.edu/security [15]
- **Cisco?s Security Vulnerability Policy** at http://www.cisco.com/c/en/us/about/security-center/security-vulnerabilit... [16]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

*/ //-->

Source URL: https://it.ucsf.edu/status/2016-08-22/cisco-released-2-critical-2-high-and-10-medium-security-updates-various-cisco

Links
[1] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepower
[2] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-fmc
[3] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-apic
[4] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp
[5] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap
[6] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap1
[7] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap2
[8] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli
[9] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepowermc
[10] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ipp
[11] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ise
[12] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-sch
[13] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ucm
[14] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-wms1
[15] http://it.ucsf.edu/security
[16] http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html