Security Update:CISCO released 2 Critical and 11 High security advisories to address vulnerabilities in multiple products

CISCO released 2 Critical and 11 High security advisories to address vulnerabilities in multiple products

Status Type

Security Update

Private

Public

Date and Time

Monday, June 11, 2018 - 12:49

Reason

Security update

Impact

Cisco users

WHAT HAPPENED

CISCO released 2 **Critical** and 11 **High** security advisories to address vulnerabilities in multiple products.

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

- **Cisco Prime Collaboration Provisioning Unauthenticated Remote Method Invocation Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-rmi

[1]

- **Cisco IOS XE Software Authentication, Authorization, and Accounting Login Authentication Remote Code Execution Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-aaa [2]
- **Cisco Web Security Appliance Layer 4 Traffic Monitor Security Bypass Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-wsa [3]
- **Cisco Prime Collaboration Provisioning SQL Injection Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-sql [4]
- **Cisco Prime Collaboration Provisioning Unauthorized Password Reset Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-password-reset [5]
- **Cisco Prime Collaboration Provisioning Unauthorized Password Recovery Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-password-recovery [6]
- **Cisco Prime Collaboration Provisioning Access Control Bypass Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-access [7]

- **Cisco Prime Collaboration Provisioning Access Control Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-wsa [3]
- **Cisco Network Services Orchestrator Arbitrary Command Execution Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-nso [8]
- **Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware Session Initiation Protocol Denial of Service Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-multiplatform-sip [9]
- **Multiple Cisco Products Disk Utilization Denial of Service Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-diskdos [10]
- **Cisco Meeting Server Information Disclosure Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-cms-id [11]
- **Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability**: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd [12]

Affected Systems:

- **Cisco Prime Collaboration Provisioning (PCP) Releases 11.6 and prior**
- **Cisco devices that are running Cisco IOS XE Software Release Fuji 16.7.1 or Fuji 16.8.1 and are configured to use AAA for login authentication**

- **Cisco AsyncOS versions for WSA on both virtual and hardware appliances running any release of the 10.5.1, 10.5.2, or 11.0.0 WSA Software**
- **Cisco Prime Collaboration Provisioning (PCP) Releases 12.2 and prior**
- **Cisco Network Services Orchestrator (NSO)**
  - **4.1 through 4.1.6.0**
  - **4.2 through 4.2.4.0**
  - **4.3 through 4.3.3.0**
  - **4.4 through 4.4.2.0**
- **Cisco IP Phone 6800, 7800, and 8800 Series Phones with Multiplatform Firmware if they are running a Multiplatform Firmware release prior to Release 11.1(2)**
- **Emergency Responder**
- **Finesse**
- **Hosted Collaboration Mediation Fulfillment**
- **MediaSense**
- **Prime License Manager**
- **SocialMiner**
- **Unified Communications Manager (UCM)**
- **Unified Communications Manager IM and Presence Service (IM&P); earlier releases were known as Cisco Unified Presence**
- **Unified Communication Manager Session Management Edition (SME)**
- **Unified Contact Center Express (UCCx)**
- **Unified Intelligence Center (UIC)**
- **Unity Connection**
- **Virtualized Voice Browser**
- **Prime Collaboration Assurance**
- **Prime Collaboration Provisioning**
- **Cisco Meeting Server (CMS) 2000 Platforms that are running a CMS Software release prior to Release 2.2.13 or Release 2.3.4**
- **3000 Series Industrial Security Appliance (ISA)**
- **ASA 1000V Cloud Firewall**
- **ASA 5500 Series Adaptive Security Appliances**
- **ASA 5500-X Series Next-Generation Firewalls**
- **ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers**
- **Adaptive Security Virtual Appliance (ASAv)**
- **Firepower 2100 Series Security Appliance**
- **Firepower 4100 Series Security Appliance**
- **Firepower 9300 ASA Security Module**
- **FTD Virtual (FTDv)**

WHAT?S THE PROBLEM?

A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

WHAT DO I NEED TO DO?

Users and administrators are encouraged to review the above Cisco Security Advisory and apply the offered updates.

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/2018-06-11/cisco-released-2-critical-and-11-high-security-advisories-address-vulnerabilities

Links
[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-rmi
[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-aaa
[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-wsa
[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-sql
[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-password-reset
[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-password-recovery
[7] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-prime-access
[8] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-nso
[9] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-multiplatform-sip
[10] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-diskdos
[11] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-cms-id
[12] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd