Alert – Multiple Vulnerabilities in Cisco Products

Description:

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for arbitrary code execution on the affected system as the logged on user. Depending on the privileges associated with the user or application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Users or applications that have been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

Systems affected:

- Cisco SD-WAN Solution prior to Release 18.4.0
- Cisco 1540 Aironet Series Outdoor Access Points prior to 8.8.100.0
- Cisco 1800i Aironet Access Points prior to 8.8.100.0
- Cisco 1810 Aironet Access Points prior to 8.8.100.0
- Cisco 1815i Aironet Access Points prior to 8.8.100.0
- Cisco 1815m Aironet Access Points prior to 8.8.100.0
- Cisco 1815w Aironet Access Points prior to 8.8.100.0
- Cisco 4800 Aironet Access Points prior to 8.8.100.0
- Meraki MR30H Access Point prior to MR 25.13
- Meraki MR33 Access Point prior to MR 25.13
- Meraki MR74 Access Point prior to MR 25.13
- Meraki MR42E Access Point prior to MR 26.1
- Meraki MR53E Access Point prior to MR 26.1
- Cisco Webex Teams prior to version 3.0.10260
- Cisco Webex Business Suite WBS32 sites — All Webex Network Recording Player and Webex Player versions prior to Version WBS32.15.33
- Cisco Webex Business Suite WBS33 sites — All Webex Network Recording Player and Webex Player versions prior to Version WBS33.6.1 or WBS 33.7.0
- Cisco Webex Meetings Online — All Webex Network Recording Player and Webex Player versions prior to Version 1.3.40
- Cisco Webex Meetings Server — All Webex Network Recording Player versions prior to Version 2.8MR3 SecurityPatch1 or 3.0MR2 SecurityPatch2
- Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers running Firmware Releases 1.4.2.15 through 1.4.2.19
- Cisco Identity Services Engine prior to 2.2.0 patch 10, prior to 2.2.1 patch 1, prior to 2.3 patch 5, and prior to 2.4 patch 2
- Connected Grid Network Management System, if running a software release prior to IoT-FND Release 3.0, prior to 4.1.2, prior to 4.3.0

- Cisco Firepower Threat Defense Software Release 6.3.0 only when running on Firepower 4100 or Firepower 9300 Series Platforms.
- Cisco Unified Intelligence Center
- Cisco AMP Threat Grid Cloud prior to 3.5.68 and Cisco AMP Threat Grid Appliance software prior to 2.5
- Cisco Enterprise NFV Infrastructure Software (NFVIS)
- Cisco SocialMiner
- Cisco Firepower Management Center
- Cisco Prime Infrastructure
- Cisco Connected Mobile Experiences (CMX) software

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **MEDIUM**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **MEDIUM**

Home Users: **LOW**

Technical Summary:

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for arbitrary code execution on the affected system as the logged on user. Details of these vulnerabilities are as follows:

- A vulnerability in the vContainer of the Cisco SD-WAN Solution could allow an authenticated remote attacker to cause a denial of service (DoS) condition and execute arbitrary code as the root user. (CVE-2019-1651)
- A vulnerability in Texas instruments chips in the affected Cisco Aironet and Meraki Access Points could allow an attacker to inject malicious Bluetooth frames to cause denial of service or remote code execution on the affected devices. (CVE-2018-16986)
- A vulnerability in the Cisco Webex Teams client formerly Cisco Spark could allow an attacker to execute arbitrary commands on a targeted system. (CVE-2019-1636)
- Multiple vulnerabilities in the Cisco Webex Network Recording Player for Microsoft Windows and the Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. (CVE-2019-1637, CVE-2019-1638, CVE-2019-1639, CVE-2019-1640, CVE-2019-1641)
- A vulnerability in the Cisco SD-WAN Solution could allow an authenticated adjacent attacker to bypass authentication and have direct unauthorized access to other vSmart containers. (CVE-2019-1647)
- A vulnerability in the user group configuration of the Cisco SD-WAN Solution could allow an authenticated local attacker to gain elevated privileges on an affected device. (CVE-2019-1648)
- A vulnerability in the Cisco SD-WAN Solution could allow an authenticated remote attacker to overwrite arbitrary files on the underlying operating system of an affected device. (CVE-2019-1650)
- Multiple vulnerabilities in the local CLI of the Cisco SD-WAN Solution could allow an authenticated local attacker to escalate privileges and modify device configuration files. (CVE-2019-1646)
- A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated remote attacker with administrative privileges on an affected device to execute arbitrary commands. (CVE-2019-1652)

- A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated remote attacker to retrieve sensitive information. (CVE-2019-1653)
- A vulnerability in the administrative web interface of Cisco Identity Services Engine (ISE) could allow an authenticated remote attacker to gain additional privileges on an affected device. (CVE-2018-15459)
- A vulnerability in the UDP protocol implementation for Cisco IoT Field Network Director (IoT-FND) could allow an unauthenticated remote attacker to exhaust system resources resulting in a denial of service (DoS) condition. (CVE-2019-1644)
- A vulnerability in the data acquisition (DAQ) component of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to bypass configured access control policies or cause a denial of service (DoS) condition. (CVE-2019-1669)
- A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. (CVE-2019-1658)
- A vulnerability in Cisco AMP Threat Grid could allow an authenticated remote attacker to access sensitive information. (CVE-2019-1657)
- A vulnerability in the CLI of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated local attacker to access the shell of the underlying Linux operating system on the affected device. (CVE-2019-1656)
- Multiple vulnerabilities in the chat feed feature of Cisco SocialMiner could allow an unauthenticated remote attacker to perform cross-site scripting (XSS) attacks against a user of the web-based user interface of an affected system. (CVE-2019-1668)
- A vulnerability in the web-based management interface of Cisco Webex Meetings Server could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface of the affected software. (CVE-2019-1655)
- Multiple vulnerabilities in the logging component of Cisco Identity Services Engine could allow an unauthenticated remote attacker to conduct cross-site scripting attacks. (CVE-2018-15455, CVE-2018-0187)
- A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) software could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. (CVE-2019-1642)
- A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. (CVE-2019-1643)
- A vulnerability in the Cisco Connected Mobile Experiences (CMX) software could allow an unauthenticated adjacent attacker to access sensitive data on an affected device. (CVE-2019-1645)

Solution:

Rw-CSIRT is strongly recommending **users** and **IT administrators** to:

- Install the update provided by Cisco immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

Affected users should: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

References:

Cisco:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-bo
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181101-ap
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-webex-teams
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-webex-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-unaccess
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-sol-escal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-file-write
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-escal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-info
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-ise-privilege
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-iot-fnd-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-firepowertds-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-uic-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-threat-grid
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-nfvis-shell-access
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-miner-chat-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-meetings-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-isel-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-ise-info-disclosure
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-frpwr-mc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-cpi-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-cmx-info-discl

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15455
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15459

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16986
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1636
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1637
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1638
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1639
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1640
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1641
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1642
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1643
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1644
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1645
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1646
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1647
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1648
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1650
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1651
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1652
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1653
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1655
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1656
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1657
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1658
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1668
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1669

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of “early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability” and raise cyber security awareness in public.