TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2019-046

DATE(S) ISSUED: 04/19/2019

SUBJECT: Multiple Vulnerabilities in Cisco Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for remote code execution on the affected system. 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.

THREAT INTELLIGENCE: There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco Catalyst Switches
- Cisco Embedded Service
- Cisco Enhanced Layer 2/3
- Cisco Gigabit Ethernet Switch Module (CGESM) for HP
- Cisco IE
- Cisco ME 4924-10GE Switch
- Cisco RF Gateway 10
- Cisco SM-X Layer 2/3 EtherSwitch Service Module
- Cisco Aironet Series Access Points
- Cisco Wireless Controllers
- Cisco Wireless LAN Controllers (WLCs)
- Cisco Expressway Series
- Cisco TelePresence Video Communication Server
- Cisco Firepower Management Center
- Cisco Email Security Appliance
- Cisco Expressway Series
- Cisco TelePresence Video Communication Server (VCS)
- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco Identity Services Engine
- Cisco Prime Network Registrar
- Cisco Registered Envelope Service
- Cisco DNA Center
- Cisco Unified Communications Manager (Unified CM)
- Cisco UCS B-Series Blade Servers
- Cisco Umbrella

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 remote code execution on the affected system. Details of these vulnerabilities are as follows:

- A vulnerability in the Cisco Cluster Management Protocol (CMP) processing code in Cisco IOS and Cisco IOS XE Software could allow an unauthenticated remote attacker to cause a reload of an affected device or remotely execute code with elevated privileges. (CVE-2017-3881) **NOTE: This vulnerability only affects devices configured to accept telnet connections.
- A vulnerability in the sysadmin virtual machine (VM) on Cisco ASR 9000 Series Aggregation Services Routers running Cisco IOS XR 64-bit Software could allow an unauthenticated remote attacker to access internal applications running on the sysadmin VM. (CVE-2019-1710)
- The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS and IOS XE Software contains multiple vulnerabilities that could allow an authenticated remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. (CVE-2017-6736, CVE-2017-6737, CVE-2017-6738, CVE-2017-6739, CVE-2017-6740, CVE-2017-6741, CVE-2017-6742, CVE-2017-6743, CVE-2017-6744)
- Multiple vulnerabilities in the handling of Inter-Access Point Protocol (IAPP) messages by Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated adjacent attacker to cause a denial of service (DoS) condition. (CVE-2019-1796, CVE-2019-1799, CVE-2019-1800)
- Multiple vulnerabilities in the administrative GUI configuration feature of Cisco Wireless LAN Controller (WLC) Software could allow an authenticated remote attacker to cause the device to reload unexpectedly during device configuration when the administrator is using this GUI causing a denial of service (DoS) condition on an affected device. The attacker would need to have valid administrator credentials on the device. (CVE-2018-0248)
- A vulnerability in the web-based management interface of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on the device with the privileges of the user including modifying the device configuration. (CVE-2019-1797)
- A vulnerability in the phone book feature of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated remote attacker to cause the CPU to increase to 100% utilization causing a denial of service (DoS) condition on an affected system. (CVE-2019-1721)
- A vulnerability in the development shell (devshell) authentication for Cisco Aironet Series Access Points (APs) running the Cisco AP-COS operating system could allow an authenticated local attacker to access the development shell without proper authentication which allows for root access to the underlying Linux OS. The attacker would need valid device credentials. (CVE-2019-1654)
- A vulnerability in certain access control mechanisms for the Secure Shell (SSH) server implementation for Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated adjacent attacker to access a CLI instance on an affected device. (CVE-2019-1805)
- A vulnerability in Locally Significant Certificate (LSC) management for the Cisco Wireless LAN Controller (WLC) could allow an authenticated remote attacker to cause the device to unexpectedly restart which causes a denial of service (DoS) condition. The attacker would need to have valid administrator credentials. (CVE-2019-1830)
- A vulnerability in the session identification management functionality of the web-based interface of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated remote attacker to hijack a valid user session on an affected system. (CVE-2018-0382)
- A vulnerability in the URL block page of Cisco Umbrella could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user in a network protected by Umbrella. (CVE-2019-1792)
- A vulnerability in the local management CLI implementation for specific commands on the Cisco UCS B-Series Blade Servers could allow an authenticated local attacker to overwrite an arbitrary file on disk.

It is also possible the attacker could inject CLI command parameters that should not be allowed for a specific subset of local management CLI commands. (CVE-2019-1725)

- A vulnerability in the User Data Services (UDS) API of Cisco Unified Communications Manager (Unified CM) could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on the management GUI. (CVE-2019-1837)
- A vulnerability in the Software Image Management feature of Cisco DNA Center could allow an authenticated remote attacker to access to internal services without additional authentication. (CVE-2019-1841)
- A vulnerability in the web-based interface of the Cisco Registered Envelope Service could allow an authenticated remote attacker to conduct a cross-site scripting (XSS) attack against another user of the service. (CVE-2019-1777)
- A vulnerability in the DHCPv6 input packet processor of Cisco Prime Network Registrar could allow an unauthenticated remote attacker to restart the server and cause a denial of service (DoS) condition on the affected system. (CVE-2019-1840, CVE-2019-1719)
- A vulnerability in the web interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated remote attacker to trigger high CPU usage resulting in a denial of service (DoS) condition. (CVE-2019-1718)
- A vulnerability in the TCP flags inspection feature for access control lists (ACLs) on Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated remote attacker to bypass protection offered by a configured ACL on an affected device. (CVE-2019-1686)
- A vulnerability in the Protocol Independent Multicast (PIM) feature of Cisco IOS XR Software could allow an unauthenticated remote attacker to cause the PIM process to restart resulting in a denial of service condition on an affected device. (CVE-2019-1712)
- A vulnerability in the Event Management Service daemon (emsd) of Cisco IOS XR Software could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-1711)
- A vulnerability in the FindMe feature of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. (CVE-2019-1722)
- A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated remote attacker to bypass configured content filters on the device. (CVE-2019-1831)
- A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. (CVE-2019-1802)
- A vulnerability in the XML API of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated remote attacker to cause the CPU to increase to 100% utilization causing a denial of service (DoS) condition on an affected system. (CVE-2019-1720)
- A vulnerability in the search path processing of Cisco Directory Connector could allow an authenticated local attacker to load a binary of their choosing. (CVE-2019-1794)
- A vulnerability in the CLI of Cisco Aironet Access Points (APs) could allow an authenticated local attacker to access sensitive information stored in an AP. (CVE-2019-1835)
- A vulnerability in the internal packet processing of Cisco Aironet Series Access Points (APs) could allow an unauthenticated adjacent attacker to cause a denial of service (DoS) condition on an affected AP if the switch interface where the AP is connected has port security configured. (CVE-2019-1834)
- A vulnerability in the CLI of Cisco Aironet Series Access Points (APs) could allow an authenticated local attacker to gain access to the underlying Linux operating system (OS) without the proper authentication. The attacker would need valid administrator device credentials. (CVE-2019-1829)
- A vulnerability in the quality of service (QoS) feature of Cisco Aironet Series Access Points (APs) could allow an authenticated adjacent attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-1826)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution on the affected system. 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.

RECOMENDATIONS:

We recommend the following actions be taken:

- 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.

REFERENCES:

Cisco:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-asr9k-exr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-iapp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-gui
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-es-tvcs-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-aironet-shell
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-ssh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-cert-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlan-hijack
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-umbrella-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ucs-cli-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ucm-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-swim-proxy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-res-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-pnr-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ise-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ise-ssl-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-iosxracl
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-iosxr-pim-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ios-xr-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ex-vcs-xsrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-esa-filter-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-cfmc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ces-tvcs-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-cdc-hijack
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-air-ap-traversal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-air-ap-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-air-ap-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-aap-dos

CVEs:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3881
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6737
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6738

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6739
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6740
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0248
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0382
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1654
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1710
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1711
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1712
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1718
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1720
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1721
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1722
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1725
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1777
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1792
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1794
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1796
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1797
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1799
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1800
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1802
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1826
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1829
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1831
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1834
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1835
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1837
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1840
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1841

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722