TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2019-050

DATE(S) ISSUED: 05/02/2019

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which 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.

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

SYSTEMS AFFECTED:

- Cisco Nexus 9000 Series Switches
- Cisco Nexus 9000 Series Fabric Switches
- Cisco Umbrella
- Cisco Small Business Switches
- Cisco Firepower Threat Defense
- Cisco Application Policy Infrastructure Controller
- Cisco Prime Collaboration Assurance
- Cisco Adaptive Security Appliance
- Clientless SSL VPN (WebVPN)
- AnyConnect Remote Access VPN
- Cisco Expressway Series
- Cisco Web Security Appliance
- Cisco Firepower 2100 Series
- Cisco Adaptive Security Virtual Appliance
- Cisco Prime Network Registrar
- Cisco Email Security Appliance
- Cisco IP Phone 7800 and 8800 Series
- Cisco HyperFlex HX-Series
- Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers

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. Details of these vulnerabilities are as follows:

- A vulnerability in the SSH key management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated remote attacker to connect to the affected system with the privileges of the root user. (CVE-2019-1804)

- A vulnerability in the log subscription subsystem of the Cisco Web Security Appliance (WSA) could allow an authenticated local attacker to perform command injection and elevate privileges to root. (CVE-2019-1816)
- A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance could allow an unauthenticated remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-1817)
- A vulnerability in the session management functionality of the web UI for the Cisco Umbrella Dashboard could allow an authenticated remote attacker to access the Dashboard via an active user session. (CVE-2019-1807)
- A vulnerability in the WebVPN login process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause increased CPU utilization on an affected device. (CVE-2018-15388)
- A vulnerability in the Secure Shell (SSH) authentication process of Cisco Small Business Switches software could allow an attacker to bypass client-side certificate authentication and revert to password authentication. (CVE-2019-1859)
- A vulnerability in the session management functionality of the web-based interface for Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated remote attacker to hijack a valid user session on an affected system. An attacker could use this impersonated session to create a new user account or otherwise control the device with the privileges of the hijacked session. (CVE-2019-1724)
- A vulnerability in the call-handling functionality of Session Initiation Protocol (SIP) Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated remote attacker to cause an affected phone to reload unexpectedly resulting in a temporary denial of service (DoS) condition. (CVE-2019-1635)
- A vulnerability in the filesystem management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated local attacker with administrator rights to gain elevated privileges as the root user on an affected device. (CVE-2019-1803)
- Multiple vulnerabilities in the Server Message Block (SMB) Protocol preprocessor detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated adjacent or remote attacker to cause a denial of service (DoS) condition. (CVE-2019-1696, CVE-2019-1704)
- A vulnerability in the internal packet-processing functionality of Cisco Firepower Threat Defense (FTD) Software for the Cisco Firepower 2100 Series could allow an unauthenticated remote attacker to cause an affected device to stop processing traffic resulting in a denial of service (DoS) condition. (CVE-2019-1703)
- A vulnerability in the TCP ingress handler for the data interfaces that are configured with management access to Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause an increase in CPU and memory usage resulting in a denial of service (DoS) condition. (CVE-2018-15462)
- A vulnerability in the implementation of Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) for Clientless SSL VPN (WebVPN) and AnyConnect Remote Access VPN in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to successfully establish a VPN session to an affected device. (CVE-2019-1714)
- A vulnerability in the software cryptography module of the Cisco Adaptive Security Virtual Appliance (ASAv) and Firepower 2100 Series running Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated remote attacker to cause an unexpected reload of the device that results in a denial of service (DoS) condition. (CVE-2019-1706)
- A vulnerability in the Internet Key Exchange Version 2 Mobility and Multihoming Protocol (MOBIKE) feature for the Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause a memory leak or a reload of an affected device that leads to a denial of service (DoS) condition. (CVE-2019-1708)
- A vulnerability in the Deterministic Random Bit Generator (DRBG), also known as Pseudorandom Number Generator (PRNG), used in Cisco Adaptive Security Appliance (ASA) Software and Cisco

Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a cryptographic collision, enabling the attacker to discover the private key of an affected device. (CVE-2019-1715)

- A vulnerability in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2019-1693)
- A vulnerability in the TCP processing engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause an affected device to reload resulting in a denial of service (DoS) condition. (CVE-2019-1694)
- A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. (CVE-2019-1713)
- A vulnerability in the FUSE filesystem functionality for Cisco Application Policy Infrastructure Controller (APIC) software could allow an authenticated local attacker to escalate privileges to root on an affected device. (CVE-2019-1682)
- A vulnerability in the Transport Layer Security (TLS) certificate validation functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated remote attacker to perform insecure TLS client authentication on an affected device. (CVE-2019-1590)
- A vulnerability in the background operations functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated local attacker to gain elevated privileges as root on an affected device. (CVE-2019-1592)
- A vulnerability in the authorization subsystem of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated but unprivileged (levels 0 and 1) remote attacker to perform privileged actions by using the web management interface. (CVE-2018-15465)
- A vulnerability in the remote access VPN session manager of Cisco Adaptive Security Appliance (ASA) Software could allow a unauthenticated remote attacker to cause a denial of service (DoS) condition on the remote access VPN services. (CVE-2019-1705)
- A vulnerability in the web-based management interface of Cisco Prime Network Registrar could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. (CVE-2019-1852)
- A vulnerability in the web-based management interface of Cisco Prime Collaboration Assurance (PCA) could allow an unauthenticated remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. (CVE-2019-1856)
- A vulnerability in the web-based management interface of Cisco HyperFlex HX-Series could allow an unauthenticated remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. (CVE-2019-1857)
- A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated local attacker to perform a command injection attack. (CVE-2019-1699)
- A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated local attacker to perform a command injection attack. (CVE-2019-1709)
- A vulnerability in the system shell for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated local attacker to use symbolic links to overwrite system files. These system files may be sensitive and should not be overwritable by non-root users. The attacker would need valid device credentials. (CVE-2019-1836)
- A vulnerability in the management web interface of Cisco Expressway Series could allow an authenticated remote attacker to perform a directory traversal attack against an affected device. (CVE-2019-1854)
- A vulnerability in certain attachment detection mechanisms of the Cisco Email Security Appliance (ESA) could allow an unauthenticated remote attacker to bypass the filtering functionality of an affected device. (CVE-2019-1844)

- A vulnerability in the TCP proxy functionality for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause the device to restart unexpectedly resulting in a denial of service (DoS) condition. (CVE-2019-1687)
- A vulnerability in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated remote attacker to cause an affected device to reload resulting in a denial of service (DoS) condition. (CVE-2019-1697)
- Multiple vulnerabilities in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the WebVPN portal of an affected device. (CVE-2019-1701)
- A vulnerability in the detection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated adjacent attacker to send data directly to the kernel of an affected device. (CVE-2019-1695)
- A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) 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 device. (CVE-2019-1838)
- A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated remote attacker to access sensitive system usage information. (CVE-2019-1692)
- A vulnerability in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated local attacker with physical access to obtain sensitive information from an affected device. (CVE-2019-1586)
- A vulnerability in the Trusted Platform Module (TPM) functionality of software for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated local attacker with physical access to view sensitive information on an affected device. (CVE-2019-1589)
- A vulnerability in Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated remote attacker to access sensitive information. (CVE-2019-1587)

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.

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-20190501-nexus9k-sshkey
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-wsa-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-wsa-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-udb-sm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-sd-cpu-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-scbv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-sbr-hijack
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-phone-sip-xml-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-rpe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-smb-snort
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-firepower-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asaftd-saml-vpn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ipsec-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-ike-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-entropy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-frpwrtd-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-apic-priv-escalation
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-insecure-fabric
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-hw-clock-util
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181219-asa-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-vpn-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-pnr-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-pca-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-hyperflex-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-ftd-cmd-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-frpwr-cmd-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-fabric-traversal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-expressway-traversal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-esa-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftdtcp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftds-ldapdos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftd-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-apic-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-apic-info-disc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-apic-encrypt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-unmeasured-boot
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-aci-filter-query

CVEs:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1586
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1587
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1589
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1590
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1592
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1635
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1682
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1687

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1693
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1694
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1695
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1696
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1697
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1699
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1703
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1704
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1705
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1706
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1709
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1713
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1724
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1804
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1836
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1844
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1852
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1854
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1856
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1857
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15388
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15462
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15465

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