TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2020-017

DATE(S) ISSUED: 02/06/2020

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco Devices, the most severe of which could allow for arbitrary code execution. Cisco is a vender for IT, networking and cybersecurity solutions. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
An undisclosed reliable exploit for CVE-2020-3119 has been crafted by Armis, Inc. There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Cisco WSA releases 12.0.1-268 and 11.8.0-382
- Cisco devices running Cisco IOS XR Software releases earlier than 6.6.3, 7.0.2, 7.1.1, or 7.2.1 and if they are configured with both the IS-IS routing protocol and SNMP versions 1, 2c, or 3
- Cisco DNA Center Software releases earlier than 1.3.0.6 and 1.3.1.4
- Cisco ISE Software releases earlier than Release 2.7.0.
- Cisco products with Cisco Discovery Protocol enabled both globally and on at least one interface and if they are running a vulnerable release of Cisco FXOS, IOS XR (32-bit or 64-bit), or NX-OS Software
    - Please review the Cisco advisory associated with CVE-2020-3120 for details in discovering if your Cisco device is vulnerable to the CVE
    - Please review the Cisco advisory associated with CVE-2020-3118 for details in discovering if your Cisco device is vulnerable to the CVE
    - Please review the Cisco advisory associated with CVE-2020-3119 for details in discovering if your Cisco device is vulnerable to the CVE
- Cisco Video Surveillance 8000 Series IP Cameras with the Cisco Discovery Protocol enabled and running a firmware version earlier than 1.0.7
- Cisco IP phones with Cisco Discovery Protocol enabled and running a vulnerable firmware release:
    - Please review the Cisco advisory associated with CVE-2020-3111 for details in discovering if your Cisco device is vulnerable to the CVE

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Cisco Products, the most severe of which could result in arbitrary code execution. These vulnerabilities can be exploited when maliciously crafted packets are sent to the vulnerable device. Details of the vulnerabilities are as follows:

- Insufficient validation of user input in the API Framework of Cisco AsyncOS for Cisco Web Security Appliance (WSA) and Cisco Content Security Management Appliance (SMA) (CVE-2020-3117)
- Improper handling of a Simple Network Management Protocol (SNMP) request for specific Object Identifiers (OIDs) by the IS-IS process in Cisco IOS XR Software (CVE-2019-16027)
- Insufficient validation of user-supplied input in the web-based management interface of Cisco Digital Network Architecture (DNA) (CVE-2019-15253)
- Insufficient input validation by the web-based management interface of Cisco Identity Services Engine (ISE) Software (CVE-2020-3149)
- Insufficient check when for Cisco FXOS, Cisco IOS XR, or Cisco NX-OS processes Cisco Discovery Protocol messages. (CVE-2020-3120)
- Improper validation of string input from certain fields in Cisco Discovery Protocol messages for Cisco IOS XR Software (CVE-2020-3118)
- Improper checks when the Cisco Video Surveillance 8000 Series IP Cameras process Cisco Discovery Protocol messages (CVE-2020-3110)
- Improper input validation for certain fields in Cisco Discovery Protocol for the Cisco NX-OS Software (CVE-2020-3119)
- Improper checks when Cisco IP Phones process Cisco Discovery Protocol messages (CVE-2020-3111)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

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

REFERENCES:

Armis:

https://go.armis.com/hubfs/White-papers/Armis-CDPwn-WP.pdf

Cisco:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-wsa-sma-header-inject

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-ios-xr-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190205-dnac-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-DxJsRWRx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15253
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16027
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3110
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3111
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3117
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3118
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3120
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3149

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

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules,
TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/