The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

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/

DATE(S) ISSUED:
1/21/2021

SUBJECT:
Multiple Vulnerabilities in Cisco Products Could Lead to Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco's SD-WAN, DNA Center, and Smart Software Manager Satellite products, the most severe of which could allow for arbitrary code execution with system privileges.

- SD-WAN is used for cloud-based network architecture
- DNA Center is a management platform for the Digital Network Architecture product
- Smart Software Manager is an enterprise product activation key/license manager

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with system privileges, with which an attacker could view, change, or delete any data.

THREAT INTELLIGENCE:
There are currently no published exploits in the wild.

SYSTEMS AFFECTED:

- Cisco IOS XE SD-WAN prior to version 16.12.4
- Cisco IOS XE Universal 17.2, 17.3, 17.4
- Cisco SD-WAN 18.X prior to version 18.4.5
- Cisco SD-WAN 19.2.X prior to version 19.2.2
- Cisco SD-WAN 19.3.0
- Cisco SD-WAN 20.1, 20.3, 20.4
- Cisco SD-WAN vBond Orchestrator
- Cisco SD-WAN vEdge Cloud Routers
- Cisco SD-WAN vEdge Routers
- Cisco SD-WAN vManage Software
- Cisco SD-WAN vSmart Controller
- DNA Center Software versions prior to 1.3.1
- Cisco Smart Software Manager Satellite versions prior to 6.3.0

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's SD-WAN, DNA Center, and Smart Software Manager Satellite products, the most severe of which could allow for arbitrary code execution in the context of the system process. Exploits can be triggered via specially crafted user input that is incorrectly validated, causing buffer overflows and command injections. Details of the vulnerabilities are as follows:

<u>SD-WAN</u>

- A buffer-overflow vulnerability that occurs due to incorrect handling of IP traffic (CVE-2021-1300)
- A buffer-overflow vulnerability that occurs due to insufficient input validation of user-supplied input that is read by the system during the establishment of an SSH connection (CVE-2021-1301)

<u>DNA Center</u>

- A command injection vulnerability that occurs due to insufficient input validation of user input within the Command Runner tool (CVE-2021-1264)

<u>Cisco Smart Software Manager Satellite</u>

- Multiple command injection vulnerabilities that occur due to insufficient input validation of user input within the web UI (CVE-2021-1138, CVE-2021-1140, CVE-2021-1142)
- Multiple command injection vulnerabilities that occur due to insufficient input validation of user input within the web UI and provide system privileges (CVE-2021-1139, CVE-2021-1141)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with system privileges, with which an attacker could view, change, or delete any data. Application of Principle of Least Privilege is only effective for vulnerabilities that do not grant system privileges.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Cisco immediately after appropriate testing.
- Block external access at the network boundary, unless external parties require service. If global access isn't needed, filter access to vulnerable hosts at the network boundary.
- Apply the Principle of Least Privilege to all systems and services; run all software as a nonprivileged user with minimal access rights.

REFERENCES:

Cisco:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-cmdinj-erumsWh9
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A

CVEs:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1300
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1301
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1264
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1138
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1140
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1142
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1139
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1141