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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
04/07/2021

SUBJECT:
Multiple Vulnerabilities in Cisco SD-WAN vManage Software Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco SD-WAN vManage Software, the most severe of which could allow for arbitrary code execution. Cisco SD-WAN provides a centralized management interface of an organization's WAN including their cloud and data center environment. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications configured to have fewer restrictions on the system could be less impacted than those who operate with elevated privileges.

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

SYSTEMS AFFECTED:
- Cisco SD-WAN vManage Release 18.4 and earlier
- Cisco SD-WAN vManage Release 19.2 and earlier
- Cisco SD-WAN vManage Release 19.3 and earlier
- Cisco SD-WAN vManage Release 20.1 and earlier
- Cisco SD-WAN vManage Release 20.3 and earlier
- Cisco SD-WAN vManage Release 20.4 and earlier

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

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

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Cisco SD-WAN vManage Software, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A vulnerability exists due to improper validation of user-supplied input in a remote management component which could allow for a buffer overflow condition leading to arbitrary code execution. (CVE-2021-1479)
- A vulnerability exists due to improper validation within a user management function could allow an authenticated, local attacker to gain escalated privileges on the underlying operating system. (CVE-2021-1137)
- A vulnerability exists due to improper validation of input to the system file transfer functions could allow an authenticated, local attacker to gain escalated privileges on the underlying operating system. (CVE-2021-1480)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of 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:
The following actions should 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-vmanage-YuTVWqy#fs

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1137
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1480
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1479