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:
05/06/2021

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 administrative functions and obtain an admin account. An attacker could then 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 SD-WAN vManage Release 18.4 and earlier
- Cisco SD-WAN vManage Release 19.2, 20.1, 20.3, 20.4 and 20.5

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

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

Home users: N/A

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 authentication checks on user-supplied input to an application messaging service which could enable administrative functions including the creation of a new administrative account. (CVE-2021-1468)
- Multiple vulnerabilities exist due to authorization checks on certain operations when operating in cluster mode. An attacker could exploit these vulnerabilities by sending crafted requests to the affected system to bypass authorization checks and gain elevated privileges within the affected system. (CVE-2021-1505, CVE-2021-1506, CVE-2021-1508)
- A vulnerability exists due to improper handling of API requests to the affected system which can lead to a denial of service (CVE-2021-1275)
- A vulnerability exists due to improper access controls on API endpoints when operating in multi-tenant mode which can lead to access of sensitive information (CVE-2021-1515)
- A vulnerability exists due to insufficient authorization checks which can lead to unauthenticated read and write access (CVE-2021-1284)
- A vulnerability exists due to insufficient validation of user-supplied input which can lead to arbitrary file overwrite (CVE-2021-1512)
- A vulnerability exists due to insufficient handling of malformed packets which can lead to a denial of service (CVE-2021-1513)
- A vulnerability exists due to insufficient input validation which can lead to arbitrary command injection (CVE-2021-1514)
- Multiple vulnerabilities exist due to absence of authentication for sensitive information when operating in cluster mode. An attacker could exploit these vulnerabilities by sending crafted requests to the affected system to view sensitive information on the affected system. (CVE-2021-1535, CVE-2021-1234)
- A vulnerability exists due to improper handling of HTTP headers which could allow for user account enumeration (CVE-2021-1486)
- A vulnerability exists due to insufficient validation of user-supplied input which can lead to execution of a stored cross-site scripting attack against users of the application web-based interface (CVE-2021-1507)

Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute administrative functions and obtain an admin account. An attacker could then view, change, or delete data; or create new accounts with full 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-sd-wan-vmanage-4TbynnhZ
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-9VZO4gfU
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-auth-bypass-65aYqcS2
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-QVszVUPy
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmanageinfdis-LKrFpbv
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmaninfdis3-OvdR6uu8
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-enumeration-64eNnDKy
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-xss-eN75jxtW

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1234
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1275
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1284
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1486
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1505
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1506
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1507
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1508
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1512
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1513
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1514
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1515
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1535

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.