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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
04/13/2022

SUBJECT:
Multiple Vulnerabilities in Citrix SD-WAN Contains Hard-Coded Credentials

OVERVIEW:
Multiple vulnerabilities have been discovered in Citrix SD-WAN. Citrix SD-WAN is a software defined Wide Area Network (WAN) which can allow for easier management of multiple networks. The most severe of these vulnerabilities contains hard-coded credentials. 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.

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

SYSTEMS AFFECTED:

- Citrix SD-WAN Standard/Premium Edition Appliance versions before 11.4.3a
- Citrix SD-WAN Center Management Console versions before 11.4.3
- Citrix SD-WAN Standard/Premium Edition Appliance versions before 11.4.1
- Citrix SD-WAN Orchestrator for On-Premises versions before 13.2.1

RISK:

Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Citrix SD-WAN. The most severe of these vulnerabilities could allow for arbitrary JavaScript code execution. Details of the vulnerabilities are as follows:

- Reflected cross site scripting (XSS) could allow for arbitrary JavaScript code execution. (CVE-2022-27505)
- Hard-coded credentials allow administrators to access the shell via the SD-WAN CLI. (CVE-2022-27506)

Successful exploitation of the most severe of these vulnerabilities contains hard-coded credentials. 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.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate updates provided by Citrix to vulnerable systems, 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 un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding 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:

We recommend the following actions be taken:

- Apply appropriate updates provided by Citrix to vulnerable systems, 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 un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding 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.