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 HyperFlex HX Software Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco HyperFlex HX software, the most severe of which could allow for arbitrary code execution. The Cisco HyperFlex HX Series is Cisco's a converged infrastructure system that integrates computing, networking and storage resources to increase efficiency and enable centralized management. This product contains a web-based interface which allows user can access to manage the device. Successful exploitation of the most severe of these vulnerabilities within the web interface could allow an unauthenticated, remote attacker to execute arbitrary code on the affected systems.

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

SYSTEMS AFFECTED:
- Cisco HyperFlex HX Release earlier than 4.0, and 4.0 prior to 4.0(2e)
- Cisco HyperFlex HX Release 4.5 prior to 4.5(1b)

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

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

Home users: N/A

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Cisco HyperFlex HX software, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A vulnerability in the web-based management interface could allow for arbitrary code execution on the affected device due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the root user. (CVE-2021-1497).
- A vulnerability in the web-based management interface could allow for arbitrary code execution on the affected device due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the tomcat8 user. (CVE-2021-1498).

Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute arbitrary code on the affected systems.

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Restrict access to the management web interface from authorized hosts.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1497
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1498