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:

06/03/2021

SUBJECT:

Multiple Vulnerabilities in Cisco Webex Network Recording Player and Cisco Webex Player Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco Webex Network Recording Player and Cisco Webex Player that could allow for arbitrary code execution. The Webex meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco Webex. The Webex Network Recording Player is an application that is used to convert Webex recording files to standard formats such as Windows Media Video, Flash or MP4. The Webex Player is an application that is used to play back and edit recorded Webex meeting files. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems with the privileges of the targeted user. Depending on the privileges associated with the targeted user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users configured to have fewer privileges 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 Webex Player versions prior to 41.2 on Windows and MacOS (CVE-2021-1503)
- Cisco Webex Network Recording Player versions prior to 41.2 on Windows and MacOS (CVE-2021-1503)
- Cisco Webex Player versions prior to 41.4 on Windows and MacOS (CVE-2021-1502)
- Cisco Webex Network Recording Player versions prior to 41.4 on Windows and MacOS (CVE-2021-1502)

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 Webex Network Recording Player and Cisco Webex Player that could allow for arbitrary code execution with the privileges of the targeted user. Details of the vulnerabilities are as follows:

- Multiple vulnerabilities exist due to an insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. (CVE-2021-1502, CVE-2021-1503)

Successful exploitation of these vulnerabilities could allow for arbitrary code execution in the context of the targeted 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-webex-player-dOJ2jOJ
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-rCFDeVj2

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1502
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1503

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.