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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/08/2019

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 which could allow an unauthenticated, remote attacker to execute arbitrary code on the system of a targeted user. 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 these vulnerabilities could allow the attacker to execute arbitrary code on the user's system. 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.

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

SYSTEMS AFFECTED:

- Cisco Webex Business Suite sites — all Webex Network Recording Player and Webex Player releases earlier than Release WBS 39.5.5
- Cisco Webex Meetings Online — all Webex Network Recording Player and Webex Player releases earlier than Release 1.3.43
- Cisco Webex Meetings Server — all Webex Network Recording Player releases earlier than Release 2.8MR3Patch3, 3.0MR2Patch4, 4.0, or 4.0MR1

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 the Cisco WebEx Network Recording Player and Cisco Webex Player which could allow an unauthenticated, remote attacker to execute arbitrary code on the system of a targeted user. An attacker could exploit these vulnerabilities by sending a user a link or email attachment containing a malicious ARF (Advanced Recording Format) or WRF (Webex Recording Format) file via a link or an email attachment and persuading the user to open the file with the affected software.

Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code on the user's system. 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-20190807-webex-player

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1924
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1925
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1926

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited