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:
03/25/2021

SUBJECT:
Multiple Vulnerabilities in Cisco Jabber Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco Jabber the most severe of which could allow for arbitrary code execution. Cisco Jabber provides instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing on any device. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications configured to have fewer restrictions 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 Jabber for Windows 12.1 versions prior to 12.1.5
- Cisco Jabber for Windows 12.5 versions prior to 12.5.4
- Cisco Jabber for Windows 12.6 versions prior to 12.6.5
- Cisco Jabber for Windows 12.7 versions prior to 12.7.4
- Cisco Jabber for Windows 12.8 versions prior to 12.8.5
- Cisco Jabber for Windows 12.9 versions prior to 12.9.5
- Cisco Jabber for MacOS 12.8 versions prior to 12.8.7
- Cisco Jabber for MacOS 12.9 versions prior to 12.9.6

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 Jabber, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities exist due to improper validation of message contents. These vulnerabilities could allow an authenticated, remote attacker to execute arbitrary code. (CVE-2021-1411, CVE-2021-1469)
- A vulnerability exists due to improper validation of message contents. This vulnerability could allow an authenticated, remote attacker to gain access to sensitive information. (CVE-2021-1417)
- A vulnerability exists due to improper validation of certificates. This vulnerability could allow an unauthenticated, remote attacker to intercept protected network traffic. (CVE-2021-1471)
- A vulnerability exists due to improper validation of message contents. This vulnerability could allow an authenticated, remote attacker to cause a DoS condition. (CVE-2021-1418)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on 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-cisco-jabber-PWrTATTC

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1411
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1417
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1418
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1469
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1471