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:
03/10/2021

SUBJECT:
Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Products, the most severe of which could allow for arbitrary code execution.

- Adobe Connect is a set of software that allows for web conferencing, remote meeting and desktop sharing.
- Adobe Creative Cloud Desktop Application allows access to a variety of Adobe products that aid in graphics design, video editing, web development, mobile application development, etc.
- Adobe Framemaker is a document processing software used to write and edit large or complex documents.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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:
- Adobe Connect version 11.0.5 and prior
- Creative Cloud Desktop Application version 5.3 and prior
- Adobe Framemaker version 2019.0.8 and prior

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

Adobe Connect

- Improper input validation error which could allow for arbitrary code execution (CVE-2021-21085).
- Reflected cross-site scripting error which could allow for arbitrary JavaScript execution in the browser (CVE-2021-21079, CVE-2021-21080, CVE-2021-21081)

Adobe Creative Cloud Desktop Application

- Arbitrary file overwrite error which could lead to arbitrary code execution (CVE-2021-21068)
- OS command injection error which could lead to arbitrary code execution (CVE-2021-21078)
- Improper input validation error which could allow for privilege escalation (CVE-2021-21069)

Adobe Framemaker

- Out-of-bounds read error which could lead to arbitrary code execution (CVE-2021-21056)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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 updates provided by Adobe 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 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:

Adobe:

https://helpx.adobe.com/security/products/framemaker/apsb21-14.html
https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html
https://helpx.adobe.com/security/products/connect/apsb21-19.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21056

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21068
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21069
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21078
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21079
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21081
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21085

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/