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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/11/2022

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.

- Character Animator is a desktop application software product that combines real-time live motion-capture with a multi-track recording system to control layered 2D puppets drawn in Photoshop or Illustrator.
- ColdFusion is a platform for building and deploying web and mobile applications..
- InDesign is a layout and page design software for print and digital media.
- Framemaker is a document processor designed for writing and editing large or complex documents.
- InCopy is a professional word processor.

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:

- Character Animator 2021 4.4.2 and earlier versions for Windows and macOS
- Character Animator 2022 22.3 and earlier versions for Windows and macOS
- ColdFusion 2018 Update 13 and earlier versions
- ColdFusion 2021 Version 3 and earlier versions

- InDesign 17.1 and earlier versions for Windows and macOS
- InDesign 16.4.1 and earlier versions for Windows and macOS
- Framemaker 2019 Release Update 8 and earlier for Windows
- Framemaker 2020 Release Update 4 and earlier for Windows
- InCopy 17.1 and earlier versions for Windows and macOS
- InCopy 16.4.1 and earlier versions for Windows and macOS

RISK:

Government:

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

Businesses:

- Large and medium business entities: **High**
- 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 Character Animator

- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2022-28819)

Adobe ColdFusion

- Cross-site Scripting (Reflected XSS), which could allow for arbitrary code execution. (CVE-2022-28818)

Adobe InDesign

- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2022-28831, CVE-2022-28833)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2022-28832)

Adobe Framemaker

- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2022-28821, CVE-2022-28822, CVE-2022-28825, CVE-2022-28826, CVE-2022-28827, CVE-2022-28828, CVE-2022-28829)

- Use After Free, which could allow for arbitrary code execution. (CVE-2022-28823, CVE-2022-28824)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2022-28830)

Adobe InCopy

- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2022-28834, CVE-2022-28836)
- Use After Free, which could allow for arbitrary code execution. (CVE-2022-28835)

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:
We recommend the following actions 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/security-bulletin.html
https://helpx.adobe.com/security/products/character_animator/apsb22-21.html
https://helpx.adobe.com/security/products/coldfusion/apsb22-22.html
https://helpx.adobe.com/security/products/indesign/apsb22-23.html
https://helpx.adobe.com/security/products/framemaker/apsb22-27.html
https://helpx.adobe.com/security/products/incopy/apsb22-28.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28819
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28823

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28833
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28836