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:

07/13/2021

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.

- Dimension is a 3D rendering and design software.
- Illustrator is a vector graphics editor and design program.
- Adobe Framemaker is a document processing software used to write and edit large or complex documents.
- Acrobat and Reader is a family of application software and Web services mainly used to create, view, and edit PDF documents.
- Bridge is a free digital asset management app. It is a mandatory component of Adobe Creative Suite, Adobe eLearning Suite, Adobe Technical Communication Suite and Adobe Photoshop CS2 through CS6.

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 Dimension 3.4 and earlier versions
- Adobe Illustrator 2021 25.2.3 and earlier versions
- Adobe Framemaker 2019 Update 8 and earlier
- Adobe Framemaker 2020 Release Update 1 and earlier
- Acrobat DC 2021.005.20054 and earlier versions
- Acrobat Reader DC 2021.005.20054 and earlier versions

- Acrobat 2020 2020.004.30005 and earlier versions
- Acrobat Reader 2020 2020.004.30005 and earlier versions
- Acrobat 2017 2017.011.30197 and earlier versions
- Acrobat Reader 2017 2017.011.30197 and earlier versions
- Adobe Bridge 11.0.2 and earlier versions

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 Dimension

- Uncontrolled Search Path Element, which could allow for arbitrary code execution. (CVE-2021-28595)

Adobe Illustrator

- Out-of-bounds write vulnerability, which could allow for arbitrary code execution. (CVE-2021-28591, CVE-2021-28592)
- Use After Free vulnerability, which could allow for arbitrary file system read. (CVE-2021-28593)

Adobe Framemaker

- Out-of-bounds write vulnerability, which could allow for arbitrary code execution. (CVE-2021-28596)

Acrobat and Reader

- Path Traversal vulnerability, which could allow for arbitrary file system read. (CVE-2021-35980, CVE-2021-28644)
- Use After Free vulnerabilities, which could allow for arbitrary code execution. (CVE-2021-28640, CVE-2021-28641, CVE-2021-28639, CVE-2021-35983, CVE-2021-35981, CVE-2021-28635)
- Type Confusion vulnerability, which could allow for arbitrary code execution. (CVE-2021-28643)
- Out-of-bounds Write vulnerability, which could allow for arbitrary file system write. (CVE-2021-28642)
- Out-of-bounds Read vulnerability, which could allow for a memory leak. (CVE-2021-28637)
- Heap-based Buffer Overflow vulnerability, which could allow for arbitrary code execution. (CVE-2021-28638)
- Uncontrolled Search Path Element vulnerability, which could allow for arbitrary code execution. (CVE-2021-28636)

- OS Command Injection vulnerability, which could allow for arbitrary code execution. (CVE-2021-28634)
- Out-of-bounds Read, vulnerability, which could allow for privilege escalation. (CVE-2021-35988, CVE-2021-35987)
- Type Confusion vulnerability, which could allow for arbitrary file system read. (CVE-2021-35986)
- NULL Pointer Dereference vulnerability, which could allow for application denial-of-service. (CVE-2021-35985, CVE-2021-35984)

Adobe Bridge

- Heap-based Buffer Overflow vulnerability, which could allow for arbitrary code execution. (CVE-2021-28624)
- Improper Input Validation vulnerability, which could allow for arbitrary code execution. (CVE-2021-35991)
- Out-of-bounds Write vulnerability, which could allow for arbitrary code execution. (CVE-2021-35989, CVE-2021-35990)
- Out-of-bounds Read vulnerability, which could allow for arbitrary file system read. (CVE-2021-35992)

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/dimension/apsb21-40.html
https://helpx.adobe.com/security/products/illustrator/apsb21-42.html
https://helpx.adobe.com/security/products/framemaker/apsb21-45.html
https://helpx.adobe.com/security/products/acrobat/apsb21-51.html
https://helpx.adobe.com/security/products/bridge/apsb21-53.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28591
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28593
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28595
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28596

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28637
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28638
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28639
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28641
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28642
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35992

TLP: WHITE
https://www.cisa.gov/tlp