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:
09/14/2021

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 XMP Toolkit SDK is a development kit for Adobe's Extensible Metadata Platform.
- Adobe Photoshop and Adobe Photoshop Elements is a graphics editor.
- Adobe Experience Manager is a content management solution for building websites, mobile apps, and forms.
- Adobe Genuine Service is a service that periodically verifies whether Adobe apps on your machine are genuine and notifies you if they are not.
- Adobe Digital Editions is an e-book reader software program.
- Adobe Premiere and Adobe Premiere Pro is a video editing software.
- Adobe Creative Cloud is a cloud service provided by Adobe where its software can be accessed all in one place.
- Adobe ColdFusion is a web application development platform.
- Adobe Framemaker is a document processing software used to write and edit large or complex documents.
- Adobe InDesign is an industry-leading layout and page design software for print and digital media.
- Adobe SVG Native viewer is a library that parses and renders SVG Native documents.
- Adobe InCopy is a professional word processor.
- Acrobat and Reader is a family of application software and Web services mainly used to create, view, and edit PDF 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 XMP-Toolkit-SDK 2021.07 and earlier versions
- Photoshop 2020 21.2.11 and earlier versions
- Photoshop 2021 22.5 and earlier versions
- Adobe Experience Manager (AEM) 6.5.9.0 and earlier versions
- Adobe Experience Manager (AEM) Cloud Service
- Adobe Genuine Service 7.3 and earlier versions
- Adobe Digital Editions 4.5.11.187646 and below
- Adobe Premiere Elements 2021 [build 19.0 (20210127.daily.2235820) and earlier]
- Photoshop Elements 2021 [build 19.0 (20210304.m.156367) and earlier]
- Creative Cloud Desktop Application 5.4 and earlier version
- ColdFusion 2018 Update 11 and earlier versions
- ColdFusion 2021 Version 1 and earlier versions
- Adobe Framemaker 2019 Update 8 and earlier
- Adobe Framemaker 2020 Release Update 2 and earlier
- Adobe InDesign 16.3.2 and earlier versions for macOS
- Adobe InDesign 16.3 and earlier versions for Windows
- Adobe SVG-Native-Viewer https://github.com/adobe/svg-native-viewer/commit/8182d14dfad5d1e10f53ed830328d7d9a3cfa96d and earlier versions for Linux
- Adobe InCopy 16.3.1 and earlier versions for macOS
- Adobe InCopy 16.3 and earlier versions for Windows
- Adobe Premiere Pro 15.4 and earlier versions
- Acrobat DC 2021.005.20060 and earlier versions for Windows
- Acrobat Reader DC 2021.005.20060 and earlier versions for Windows
- Acrobat DC 2021.005.20058 and earlier versions for macOS
- Acrobat Reader DC 2021.005.20058 and earlier versions for macOS
- Acrobat 2020 2020.004.30006 and earlier versions
- Acrobat Reader 2020 2020.004.30006 and earlier versions
- Acrobat 2017 2017.011.30199 and earlier versions
- Acrobat Reader 2017 2017.011.30199 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 XMP-Toolkit-SDK

- Out-of-bounds Read, which could allow for Arbitrary file system read. (CVE-2021-40716)

Adobe Photoshop 2020 and 2021

- Buffer Overflow, which could allow for Arbitrary code execution. (CVE-2021-40709)

Adobe Experience Manager (AEM)

- Cross-site Scripting (XSS), which could allow for Arbitrary code execution. (CVE-2021-40711)
- Improper Input Validation, which could allow for Application denial-of-service. (CVE-2021-40712)
- Improper Certificate Validation, which could allow for Security feature bypass. (CVE-2021-40713)
- Cross-site Scripting (XSS), which could allow for Arbitrary code execution. (CVE-2021-40714)

Adobe Genuine Service

- Creation of Temporary File in Directory with Incorrect Permissions, which could allow for Privilege Escalation. (CVE-2021-40708)

Adobe Digital Editions

- Creation of Temporary File in Directory with Incorrect Permissions, which could allow for Privilege Escalation. (CVE-2021-39828)
- Creation of Temporary File in Directory with Incorrect Permissions, which could allow for Arbitrary file system write. (CVE-2021-39827)
- OS Command Injection, which could allow for Arbitrary code execution. (CVE-2021-39826)

Adobe Premiere Elements

- Access of Memory Location After End of Buffer, which could allow for Arbitrary code execution. (CVE-2021-39824, CVE-2021-40701, CVE-2021-40700, CVE-2021-40703, CVE-2021-40702)

Adobe Photoshop Elements

- Out-of-bounds Write, which could allow for Arbitrary code execution. (CVE-2021-39825)

Creative Cloud Desktop Application

- Creation of Temporary File in Directory with Incorrect Permissions, which could allow for Arbitrary file system write. (CVE-2021-28613)

Adobe ColdFusion

- Use of Inherently Dangerous Function which could allow for Security feature bypass . (CVE-2021-40698)
- Improper Access Control which could allow for Security feature bypass. (CVE-2021-40699)

Adobe Framemaker

- Use After Free, which could allow for Arbitrary file system read. (CVE-2021-39835, CVE-2021-39833, CVE-2021-39834)
- Out-of-bounds Read, which could allow for Arbitrary file system read. (CVE-2021-40697)
- Access of Memory Location After End of Buffer, which could allow for Arbitrary code execution. (CVE-2021-39832, CVE-2021-39830)

- Out-of-bounds Write, which could allow for Arbitrary code execution. (CVE-2021-39829, CVE-2021-39831)

Adobe InDesign
- Access of Memory Location After End of Buffer, which could allow for Arbitrary code execution. (CVE-2021-39820)
- Out-of-bounds Read, which could allow for Arbitrary code execution. (CVE-2021-39821, CVE-2021-39822)

Adobe SVG-Native-Viewer
- Heap-based Buffer Overflow, which could allow for Arbitrary code execution. (CVE-2021-39823)

Adobe InCopy
- Access of Memory Location After End of Buffer, which could allow for Arbitrary file system write. (CVE-2021-39819)
- Access of Memory Location After End of Buffer, which could allow for Arbitrary code execution. (CVE-2021-39818)

Adobe Premiere Pro
- Access of Memory Location After End of Buffer, which could allow for Arbitrary Code Execution. (CVE-2021-40710, CVE-2021-40715)

Adobe Acrobat and Reader
- Type Confusion, which could allow for Arbitrary code execution. (CVE-2021-39841)
- Heap-based Buffer Overflow, which could allow for Arbitrary code execution. (CVE-2021-39863)
- Information Exposure, which could allow for Arbitrary file system read. (CVE-2021-39857, CVE-2021-39856, CVE-2021-39855)
- Out-of-bounds Read, which could allow for a Memory leak. (CVE-2021-39844, CVE-2021-39861)
- Out-of-bounds Read, which could allow for Arbitrary file system read. (CVE-2021-39858)
- Out-of-bounds Write, which could allow for a Memory leak. (CVE-2021-39843)
- Stack-based Buffer Overflow, which could allow for Arbitrary code execution. (CVE-2021-39846, CVE-2021-39845)
- Uncontrolled Search Path Element, which could allow for Arbitrary code execution. (CVE-2021-35982)
- Use After Free, which could allow for Arbitrary code execution. (CVE-2021-39859, CVE-2021-39840, CVE-2021-39842, CVE-2021-39839, CVE-2021-39838, CVE-2021-39837, CVE-2021-39836)
- NULL Pointer Dereference, which could allow for a Memory leak. (CVE-2021-39860)
- NULL Pointer Dereference, which could allow for Application denial-of-service. (CVE-2021-39852, CVE-2021-39854, CVE-2021-39853, CVE-2021-39850, CVE-2021-39849, CVE-2021-39851)

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.html
https://helpx.adobe.com/security/products/xmpcore/apsb21-85.html
https://helpx.adobe.com/security/products/photoshop/apsb21-84.html
https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html
https://helpx.adobe.com/security/products/integrity_service/apsb21-81.html
https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html
https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html
https://helpx.adobe.com/security/products/photoshop_elements/apsb21-77.html
https://helpx.adobe.com/security/products/creative-cloud/apsb21-76.html
https://helpx.adobe.com/security/products/coldfusion/apsb21-75.html
https://helpx.adobe.com/security/products/framemaker/apsb21-74.html
https://helpx.adobe.com/security/products/indesign/apsb21-73.html
https://helpx.adobe.com/security/products/svg-native-viewer/apsb21-72.html
https://helpx.adobe.com/security/products/incopy/apsb21-71.html
https://helpx.adobe.com/security/products/premiere_pro/apsb21-67.html
https://helpx.adobe.com/security/products/acrobat/apsb21-55.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28613
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39819
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39820
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39836
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39837
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39839

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39842
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39843
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39845
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39846
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39849
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39850
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39851
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39853
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39854
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39855
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39856
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39863
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40697
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40699
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40709
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40710
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40711
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40713
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40714
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40716

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