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:
12/14/2021

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.

- Premiere Rush is a video editor.
- Experience Manager is a comprehensive content management solution for building websites, mobile apps and forms.
- Connect is a suite of software for remote training, web conferencing, presentation, and desktop sharing.
- Photoshop is a graphics editor.
- Prelude software is a video ingest and logging tool that helps you quickly tag and transcode raw footage from file-based cameras.
- After Effects is a graphics and visual effects software.
- Dimension is a 3D rendering and design software
- Premiere Pro is a video editing and manipulation software.
- Media Encoder is software that provides media content over the internet.
- Lightroom is an image organization and manipulation tool.
- Audition is a professional audio editing application that includes a non-destructive mixing and editing environment.

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 Premiere Rush 1.5.16 and earlier versions for Windows
- Adobe Experience Manager 6.5.10.0 and earlier versions for all platforms

- Adobe Connect 11.3 and earlier versions for all platforms
- Adobe Photoshop 2021 22.5.3 and earlier versions for Windows and macOS
- Adobe Photoshop 2022 23.0.2 and earlier versions for Windows and macOS
- Adobe Prelude 22.0 and earlier versions for Windows
- Adobe After Effects 22.0 and earlier versions for Windows and macOS
- Adobe After Effects 18.4.2 and earlier versions for Windows and macOS
- Adobe Dimension 3.4.3 and earlier versions for Windows and macOS
- Adobe Premiere Pro 22.0 and earlier versions for Windows and macOS
- Adobe Premiere Pro 15.4.2 and earlier versions for Windows and macOS
- Adobe Media Encoder 22.0 and earlier versions for Windows and macOS
- Adobe Media Encoder 15.4.2 and earlier versions for Windows and macOS
- Adobe Lightroom 4.4 and earlier versions for Windows
- Adobe Audition 22.0 and earlier versions for Windows and macOS
- Adobe Audition 14.4 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 Premiere Rush
- Access of Memory Location After End of Buffer, which could allow for arbitrary code execution. (CVE-2021-40783, CVE-2021-40784, CVE-2021-43021, CVE-2021-43022, CVE-2021-43023, CVE-2021-43024, CVE-2021-43025, CVE-2021-43026, CVE-2021-43028, CVE-2021-43029, CVE-2021-43747)
- Access of Uninitialized Pointer, which could allow for privilege escalation. (CVE-2021-43030)
- Improper Input Validation, which could allow for arbitrary code execution. (CVE-2021-43746)
- NULL Pointer Dereference, which could allow for application denial-of-service. (CVE-2021-43748, CVE-2021-43749, CVE-2021-43750)

Adobe Experience Manager
- Cross-site Scripting (XSS), which could allow for Arbitrary code execution. (CVE-2021-43761, CVE-2021-43764)
- Improper Restriction of XML External Entity Reference ('XXE'), which could allow for Arbitrary code execution. (CVE-2021-40722)
- Improper Input Validation, which could allow for Security feature bypass. (CVE-2021-43762)
- Cross-site Scripting (Stored XSS), which could allow for Arbitrary code execution. (CVE-2021-43765, CVE-2021-44176, CVE-2021-44177)

- Cross-site Scripting (Reflected XSS), which could allow for Arbitrary code execution. (CVE-2021-44178)

Adobe Connect
- Cross-Site Request Forgery (CSRF), which could allow for arbitrary file system write. (CVE-2021-43014)

Adobe Photoshop
- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2021-43018)
- Access of Memory Location After End of Buffer, which could allow for a memory leak. (CVE-2021-43020)
- Buffer Overflow, which could allow for arbitrary code execution. (CVE-2021-44184)

Adobe Prelude
- Access of Memory Location After End of Buffer, which could allow for arbitrary code execution. (CVE-2021-43754)
- Out-of-bounds Read, which could allow for Privilege escalation. (CVE-2021-44696)

Adobe After Effects
- Access of Memory Location After End of Buffer, which could allow for arbitrary code execution. (CVE-2021-43755)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2021-44188)
- Use After Free, which could allow for privilege escalation. (CVE-2021-44189)
- Out-of-bounds Read, which could allow for privilege escalation. (CVE-2021-44190, CVE-2021-44191, CVE-2021-44192, CVE-2021-44193, CVE-2021-44194, CVE-2021-44195, CVE-2021-43027)

Adobe Dimension
- Out-of-bounds Read, which could allow for privilege escalation. (CVE-2021-43763)
- Access of Memory Location After End of Buffer, which could allow for arbitrary code execution. (CVE-2021-44179)
- Out-of-bounds Write, which could allow for arbitrary code execution. (CVE-2021-44180, CVE-2021-44181, CVE-2021-44182, CVE-2021-44183)

Adobe Premiere Pro
- Out-of-bounds Read, which could allow for privilege escalation. (CVE-2021-43751, CVE-2021-40791, CVE-2021-40795, CVE-2021-42265)
- Use After Free, which could allow for privilege escalation. (CVE-2021-40790)

Adobe Media Encoder
- Access of Memory Location After End of Buffer, which could allow for arbitrary code execution. (CVE-2021-43756)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2021-43757, CVE-2021-43758, CVE-2021-43759, CVE-2021-43760)

Adobe Lightroom
- Use After Free, which could allow for privilege escalation. (CVE-2021-43753)

Adobe Audition

- Out-of-bounds Read, which could allow for privilege escalation. (CVE-2021-44697, CVE-2021-44698, CVE-2021-44699)

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/security-bulletin.html
https://helpx.adobe.com/security/products/premiere_rush/apsb21-101.html
https://helpx.adobe.com/security/products/experience-manager/apsb21-103.html
https://helpx.adobe.com/security/products/connect/apsb21-112.html
https://helpx.adobe.com/security/products/photoshop/apsb21-113.html
https://helpx.adobe.com/security/products/prelude/apsb21-114.html
https://helpx.adobe.com/security/products/after_effects/apsb21-115.html
https://helpx.adobe.com/security/products/dimension/apsb21-116.html
https://helpx.adobe.com/security/products/premiere_pro/apsb21-117.html
https://helpx.adobe.com/security/products/media-encoder/apsb21-118.html
https://helpx.adobe.com/security/products/lightroom/apsb21-119.html
https://helpx.adobe.com/security/products/audition/apsb21-121.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40722
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40791
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42265
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43023

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43747
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43753
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43755
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43756
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44178
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44179
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44180
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44188
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44189
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44191
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44192
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44195
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44697
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44699

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