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:
06/09/2021

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.

- Connect is a suite of software for remote training, web conferencing, presentation, and desktop sharing.
- Acrobat and Reader is a family of application software and Web services mainly used to create, view, and edit PDF documents.
- Experience Manager is a content management solution for building websites, mobile apps, and forms.
- Creative Cloud is a cloud service provided by Adobe where its software can be accessed all in one place
- RoboHelp Server is a help authoring tool
- Photoshop Elements and Photoshop is a photo editing software
- Premiere is a video editing software
- After Effects is a graphics and visual effects software
- Animate is a multimedia authoring computer animation program.

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 11.2.1 and earlier versions
- Acrobat DC and Acrobat Reader DC version 2021.001.20155 and earlier
- Acrobat 2020 and Acrobat Reader 2020 version 2020.001.30025 and earlier

- Acrobat 2017 and Acrobat Reader 2017 version 2017.011.30196 and earlier
- Photoshop 2020 21.2.8 and earlier versions
- Photoshop 2021 22.4.1 and earlier versions
- Adobe Experience Manager (AEM) 6.5.8.0 and earlier versions
- Adobe Experience Manager (AEM) Cloud Services
- Creative Cloud Desktop Application (Installer) 2.4 and earlier version
- RoboHelp Server 2019.0.9 and earlier versions
- Photoshop Elements (installer) 5.2 and earlier versions
- Adobe Premiere Elements (installer) 5.2 and earlier versions
- Adobe After Effects 18.2 and earlier versions
- Adobe Animate 21.0.6 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 Connect

- Improper Access Control vulnerability, which could allow for privilege escalation (CVE-2021-28579)

Adobe Acrobat and Reader

- Out-of-bounds read vulnerability, which could allow arbitrary code execution. (CVE-2021-28554, CVE-2021-28551)
- Use After Free vulnerabilities, which could allow for arbitrary code execution. (CVE-2021-28552, CVE-2021-28631, CVE-2021-28632)

Adobe Photoshop

- Heap-based Buffer Overflow, which could allow for arbitrary code execution. (CVE-2021-28624)
- Buffer Overflow, which could allow for arbitrary code execution. (CVE-2021-28582)

Adobe Experience Manager

- Cross-site scripting vulnerability, which could allow for arbitrary code execution. (CVE-2021-28625)
- Improper Authorization vulnerability, which could allow for application denial-of-service. (CVE-2021-28626)
- Server-Side Request Forgery vulnerability, which could allow for security feature bypass. (CVE-2021-28627)
- Cross-site scripting vulnerability, which could allow for arbitrary code execution. (CVE-2021-28628)

Adobe Creative Cloud

- Creation of Temporary File in Directory with Incorrect Permissions vulnerability, which could allow for arbitrary file system write. (CVE-2021-28633)
- Uncontrolled Search Path Element vulnerability, which could allow for arbitrary code execution. (CVE-2021-28594)

Adobe RoboHelp

- Path Traversal vulnerability, which could allow for arbitrary code execution. (CVE-2021-28588)

Adobe Photoshop Elements

- Creation of Temporary File in Directory with Incorrect Permissions vulnerability, which could allow for privilege escalation (CVE-2021-28597)

Adobe Premiere Elements

- Creation of Temporary File in Directory with Incorrect Permissions vulnerability, which could allow for privilege escalation (CVE-2021-28623)

Adobe After Effects

- Out-of-bounds Read vulnerability, which could allow for memory leak (CVE-2021-28600)
- NULL Pointer Dereference vulnerability, which could allow for application denial-of-service (CVE-2021-28601)
- Access of Memory Location After End of Buffer vulnerability, which could allow for arbitrary code execution (CVE-2021-28602, CVE-2021-28605, CVE-2021-28607)
- Heap-based Buffer Overflow vulnerability, which could allow for arbitrary code execution (CVE-2021-28603, CVE-2021-28604, CVE-2021-28608, CVE-2021-28610)
- Stack-based Buffer Overflow vulnerability, which could allow for arbitrary code execution (CVE-2021-28606)
- Out-of-bounds Read vulnerability, which could allow for arbitrary file system read (CVE-2021-28609, CVE-2021-28615)
- Out-of-bounds Read vulnerability, which could allow for memory leak (CVE-2021-28611, CVE-2021-28612, CVE-2021-28614, CVE-2021-28616)

Adobe Animate

- Out-of-bounds Read vulnerability, which could allow for arbitrary file system read (CVE-2021-28630)
- Out-of-bounds Read vulnerability, which could allow for memory leak (CVE-2021-28619)
- Out-of-bounds Read vulnerability, which could allow for information disclosure (CVE-2021-28617, CVE-2021-28618)
- Out-of-bounds Read vulnerability, which could allow for arbitrary code execution (CVE-2021-28621)
- Heap-based Buffer Overflow vulnerability, which could allow for arbitrary code execution (CVE-2021-28620, CVE-2021-28629)
- Out-of-bounds Write vulnerability, which could allow for arbitrary code execution (CVE-2021-28622)

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/connect/apsb21-36.html
https://helpx.adobe.com/security/products/acrobat/apsb21-37.html
https://helpx.adobe.com/security/products/photoshop/apsb21-38.html
https://helpx.adobe.com/security/products/experience-manager/apsb21-39.html
https://helpx.adobe.com/security/products/creative-cloud/apsb21-41.html
https://helpx.adobe.com/security/products/robohelp-server/apsb21-44.html
https://helpx.adobe.com/security/products/photoshop_elements/apsb21-46.html
https://helpx.adobe.com/security/products/premiere_elements/apsb21-47.html
https://helpx.adobe.com/security/products/after_effects/apsb21-49.html
https://helpx.adobe.com/security/products/animate/apsb21-50.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28551
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28552
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28554
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28582
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28594
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28597
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28600
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28601
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28602
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28603
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28604
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28606
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28607
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28608
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28609
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28610
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28611
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28612

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28614
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28615
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28616
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28619
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28622
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28623
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28627
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28630
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28631
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28632
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28633

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.