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:
09/13/2022

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.

- Experience Manager is a comprehensive content management solution for building websites, mobile apps and forms
- Bridge is a digital asset management application
- InDesign is an industry-leading layout and page design software for print and digital media
- Photoshop is a graphics editor
- Adobe InCopy is a professional word processor.
- Animate is a multimedia authoring computer animation program.
- Illustrator is a vector graphics editor and design 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 Experience Manager 6.5.13.0 and earlier versions
- Adobe Bridge 12.0.2 and earlier versions
- Adobe Bridge 11.1.3 and earlier versions

- Adobe InDesign 17.3 and earlier versions
- Adobe InDesign 16.4.2 and earlier versions
- Adobe Photoshop 2021 22.5.8 and earlier versions
- Adobe Photoshop 2022 23.4.2 and earlier versions
- Adobe InCopy 17.3 and earlier versions
- Adobe InCopy 16.4.2 and earlier versions
- Adobe Animate 2021 21.0.11 and earlier versions
- Adobe Animate 2022 22.0.7 and earlier versions
- Adobe Illustrator 2022 26.4 and earlier versions
- Adobe Illustrator 2022 25.4.7 and earlier versions

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

Tactic: *Execution* **(**TA0002**)**:

Technique: *Exploitation for Client Execution* **(**T1203**)**

Technique: *User Execution* **(**T1204**)**

Adobe Experience Manager

- Cross-site Scripting which could result in Arbitrary code execution (CVE-2022-30677, CVE-2022-30678, CVE-2022-30680, CVE-2022-30681, CVE-2022-30682, CVE-2022-30684, CVE-2022-30685, CVE-2022-30686, CVE-2022-35664, CVE-2022-34218)
- Violation of Secure Design Principles which could result in a Security feature bypass (CVE-2022-30683)

Adobe Bridge

- Out-of-bounds Write which could result in Arbitrary code execution. (CVE-2022-35699, CVE-2022-35700, CVE-2022-35701)
- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2022-35702, CVE-2022-35703, CVE-2022-35705, CVE-2022-35707)
- Use After Free which could result in Arbitrary code execution. (CVE-2022-35704)
- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2022-35706, CVE-2022-35708)
- Use After Free which could result in a Memory Leak. (CVE-2022-35709, CVE-2022-38425)

Adobe InDesign

- Improper Input Validation which could result in an Arbitrary file system read (CVE-2022-28851)
- Out-of-bounds Write which could result in Arbitrary code execution. (CVE-2022-28852, CVE-2022-28853)
- Out-of-bounds Read which could result in Memory Leak. (CVE-2022-28854, CVE-2022-28855, CVE-2022-28856, CVE-2022-28857, CVE-2022-30671, CVE-2022-30672, CVE-2022-30673, CVE-2022-30674, CVE-2022-30675, CVE-2022-30676)
- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2022-38414, CVE-2022-38415)
- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2022-38416, CVE-2022-38417)

Adobe Photoshop

- Out-of-bounds Write which could result Arbitrary code execution. (CVE-2022-35713)
- Access of Uninitialized Pointer which could result Arbitrary code execution. (CVE-2022-38426, CVE-2022-38427)
- Use After Free which could result in Memory Leak. (CVE-2022-38428)
- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2022-38429, CVE-2022-38430, CVE-2022-38431)
- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2022-38432, CVE-2022-38433)
- Use After Free which could result in Arbitrary code execution. (CVE-2022-38434)

Adobe InCopy

- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2022-38401, CVE-2022-38404, CVE-2022-38405)
- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2022-38402, CVE-2022-38403, CVE-2022-38406, CVE-2022-38407)

Adobe Animate

- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2022-38411, CVE-2022-38412)

Adobe Illustrator

- Improper Input Validation which could result in an Arbitrary code execution. (CVE-2022-38408)
- Out-of-bounds Read which could result in a Memory Leak (CVE-2022-38409, CVE-2022-38410)

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:

- Apply the stable channel update provided by Adobe to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- 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. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example

implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048 : Application Isolation and Sandboxing**)
    - **Safeguard 4.1 : Establish and Maintain a Secure Configuration Process:** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Adobe:https://helpx.adobe.com/security/security-bulletin.html

https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html

https://helpx.adobe.com/security/products/bridge/apsb22-49.html

https://helpx.adobe.com/security/products/indesign/apsb22-50.html

https://helpx.adobe.com/security/products/photoshop/apsb22-52.html

https://helpx.adobe.com/security/products/incopy/apsb22-53.html

https://helpx.adobe.com/security/products/animate/apsb22-54.html

https://helpx.adobe.com/security/products/illustrator/apsb22-55.html

CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28851

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28852

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28853

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28854

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28855

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28856

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28857

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30671

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30672

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30673

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30674

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30675

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30676

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30677

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30680

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30681

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30682

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30682

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30683

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30684

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30685

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30686

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34218

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35664

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35699

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35700

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35701

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35702

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35703

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35704

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35705

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35706

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35707

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35708

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35709

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35713

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38401

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38402

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38403

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38404

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38405

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38406

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38407

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38408

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38409

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38410

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38411

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38412

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38414

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38415

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38416

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38417

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38425

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38426

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38427

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38428

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38429

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38430

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38431

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38432

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38433

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38434