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:
10/22/2022

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.

- Adobe ColdFusion is a web-application development computing platform.

- Adobe Acrobat Reader software is a trusted standard for viewing, printing, signing, sharing and annotating PDFs.

- Adobe Commerce connects shopping experiences across channels, add new brands and sites, expand into new geographies – all from one platform.

- Adobe Dimension is a 3D rendering and design software.

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 ColdFusion 2018
- Adobe ColdFusion 2021
- Adobe Acrobat DC 22.002.20212 and earlier versions
- Adobe Acrobat Reader DC 22.002.20212 and earlier versions
- Adobe Acrobat 2020 20.005.30381 and earlier versions
- Adobe Reader 2020 20.005.30381 and earlier versions
- Adobe Commerce 2.4.4-p1 and earlier versions
- Adobe Commerce 2.4.5 and earlier versions
- Magento Open Source 2.4.4-p1 and earlier versions
- Magento Open Source 2.4.5 and earlier versions
- Adobe Dimension 3.4.5 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 ColdFusion

• Stack-based Buffer Overflow which could result in Arbitrary code execution (CVE-2022-35710, CVE-2022-35690)

• Heap-based Buffer Overflow which could result in Arbitrary code execution (CVE-2022-35711, CVE-2022-35712)

• Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') which could result in Arbitrary code execution (CVE-2022-38418, CVE-2022-38421)

• Improper Restriction of XML External Entity Reference ('XXE') which could result in Arbitrary file system read (CVE-2022-38419, CVE-2022-42341)

• Use of Hard-coded Credentials which could result in Privilege escalation (CVE-2022-38420)

• Information Exposure which could result in Security feature bypass (CVE-2022-38422)

• Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') which could result in Security feature bypass (CVE-2022-38423)

• Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') which could result in Arbitrary file system write (CVE-2022-38424)

• Improper Input Validation which could result in Arbitrary file system read (CVE-2022-42340)

Adobe Acrobat and Reader

• NULL Pointer Dereference which could result in Application denial-of-service (CVE-2022-35691)

• Use After Free which could result in Memory leak (CVE-2022-38437)

• Stack-based Buffer Overflow which could result in Arbitrary code execution (CVE-2022-38450, CVE-2022-42339)

• Out-of-bounds Read which could result in Memory leak (CVE-2022-38449, CVE-2022-42342)

Adobe Commerce

• Cross-site Scripting (Stored XSS) which could result in an Arbitrary code execution (CVE-2022-35698)

Adobe Dimension

• Out-of-bounds Read which could result in Arbitrary code execution (CVE-2022-38440, CVE-2022-38441)

• Out-of-bounds Read which could result in Memory leak (CVE-2022-38443)

• Use After Free which could result in Arbitrary code execution (CVE-2022-38442, CVE-2022-38444, CVE-2022-38445, CVE-2022-38446, CVE-2022-38447, CVE-2022-38448)

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**)

o **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.

o **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**)

o **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.

o **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)

o **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.

o **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)

o **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.

o **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.

o **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)

o **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) o **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.

o **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/coldfusion/apsb22-44.html

https://helpx.adobe.com/security/products/acrobat/apsb22-46.html

https://helpx.adobe.com/security/products/magento/apsb22-48.html

https://helpx.adobe.com/security/products/dimension/apsb22-57.html

CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35690

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35691

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35698

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35710

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35711

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35712

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38418

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38419

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38420

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38421

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38422

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38423 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38424

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38437

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38440

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38441

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38442

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38443

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38444

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38445

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38446

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38447

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38448

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38449

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38450

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42339

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42340

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42341

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42342