MS-ISAC®
Multi-State Information Sharing & Analysis Center®

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-032

DATE(S) ISSUED:
03/14/2023

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution.

- Adobe Commerce is a platform for delivering eCommerce capabilities, including out-of-the-box features, an ability to customize, and third-party integrations.
- Adobe Experience Manager Forms is an end-to-end digital document solution that makes it easy to create responsive forms that customers can easily complete and securely e-sign.
- Adobe Illustrator is a vector graphics editor and design program.
- Adobe Dimension is a 3D rendering and design software.
- Adobe Creative Cloud is a collection of software for graphic design, video editing, web development, and photography.
- Adobe Substance 3D Stager is a state-of-the-art staging tool to create 3D scenes with real-time 3D visualization and high-quality renders.
- Adobe Photoshop is a raster graphics editor.
- Adobe ColdFusion is a commercial rapid web-application development computing platform.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. 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:
Adobe is aware that CVE-2023-26360 has been exploited in the wild in very limited attacks targeting Adobe ColdFusion.

SYSTEMS AFFECTED:

- Adobe Commerce 2.4.4-p2 and earlier versions
- Adobe Commerce 2.4.4-p1 and earlier versions
- Magento Open Source 2.4.4-p2 and earlier versions
- Magento Open Source 2.4.4-p1 and earlier versions
- Adobe Experience Manager (AEM) AEM Cloud Service (CS)
- Adobe Experience Manager (AEM) 6.5.15.0 and earlier versions
- Illustrator 2023 27.2.0 and earlier versions for Windows and macOS
- Adobe Dimension 3.4.7 and earlier versions for Windows and macOS
- Creative Cloud Desktop Application 5.9.1 and earlier version for Windows
- Adobe Substance 3D Stager 2.0.0 and earlier versions for Windows and macOS
- Photoshop 2022 23.5.3 and earlier versions for Windows and macOS
- Photoshop 2023 24.1.1 and earlier versions for Windows and macOS
- ColdFusion 2018 Update 15 and earlier versions
- ColdFusion 2021 Update 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**):**

Adobe Commerce:

- XML Injection (aka Blind XPath Injection) which could result in Arbitrary file system read. (CVE-2023-22247)
- Cross-site Scripting (Stored XSS) which could result in Arbitrary code execution. (CVE-2023-22249)
- Improper Access Control which could result in Security feature bypass. (CVE-2023-22250)
- Improper Authorization which could result in Security feature bypass. (CVE-2023-22251)

Adobe Experience Manager

- Cross-site Scripting (Reflected XSS) which could result in Arbitrary code execution. (CVE-2023-22252, CVE-2023-22253, CVE-2023-22254)
- URL Redirection to Untrusted Site ('Open Redirect') which could result in Security feature bypass. (CVE-2023-22256, CVE-2023-22257, CVE-2023-22258, CVE-2023-22259, CVE-2023-22260, CVE-2023-22261, CVE-2023-22262, CVE-2023-22263, CVE-2023-22264, CVE-2023-22265, CVE-2023-22266)
- Cross-site Scripting (Stored XSS) which could result in Arbitrary code execution. (CVE-2023-22269, CVE-2023-21615, CVE-2023-21616)
- Weak Cryptography for Passwords which could result in Privilege escalation. (CVE-2023-22271)

Adobe Illustrator

- Improper Input Validation which could result in Arbitrary code execution. (CVE-2023-25859)
- Out-of-bounds Write which could result in Arbitrary code execution. (CVE-2023-25860, CVE-2023-25861)
- Out-of-bounds Read which could result in Memory Leak. (CVE-2023-25862)
- Use After Free which could result in Arbitrary code execution. (CVE-2023-26426)

Adobe Dimension

- Improper Input Validation which could result in Arbitrary code execution. (CVE-2023-25879, CVE-2023-25881)
- Out-of-bounds Write which could result in Arbitrary code execution. (CVE-2023-25880, CVE-2023-25905, CVE-2023-26328, CVE-2023-26330)
- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2023-25882, CVE-2023-25883, CVE-2023-25885, CVE-2023-25890, CVE-2023-25895, CVE-2023-25897, CVE-2023-25898)
- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2023-25884, CVE-2023-25886, CVE-2023-25887, CVE-2023-25888, CVE-2023-25889, CVE-2023-25891, CVE-2023-25892, CVE-2023-25900, CVE-2023-25902, CVE-2023-25904, CVE-2023-25906, CVE-2023-25907, CVE-2023-26327, CVE-2023-26333, CVE-2023-26335)
- Use After Free which could result in Arbitrary code execution. (CVE-2023-25893, CVE-2023-25894, CVE-2023-25896, CVE-2023-25899, CVE-2023-26336)
- Improper Input Validation which could result in Arbitrary code execution. (CVE-2023-25901)
- Integer Overflow or Wraparound which could result in Arbitrary code execution. (CVE-2023-25903)
- Out-of-bounds Read which could result in a Memory leak. (CVE-2023-26329, CVE-2023-26331, CVE-2023-26332, CVE-2023-26338, CVE-2023-26339, CVE-2023-26340, CVE-2023-26341, CVE-2023-26342, CVE-2023-26343, CVE-2023-26344, CVE-2023-26345, CVE-2023-26346, CVE-2023-26348, CVE-2023-26350, CVE-2023-26351, CVE-2023-26352, CVE-2023-26353, CVE-2023-26354, CVE-2023-26355, CVE-2023-26356)
- Access of Uninitialized Pointer which could result in a Memory leak. (CVE-2023-26334)

- Stack-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2023-26337)
- Use After Free which could result in a Memory leak. (CVE-2023-26349)

Adobe Creative Cloud

- Untrusted Search Path which could result in Arbitrary code execution. (CVE-2023-26358)

Adobe Substance 3D Stager

- Out-of-bounds Read which could result in Arbitrary code execution. (CVE-2023-25863, CVE-2023-25869, CVE-2023-25873)
- Heap-based Buffer Overflow which could result in Arbitrary code execution. (CVE-2023-25864, CVE-2023-25868, CVE-2023-25872, CVE-2023-25874)
- Access of Memory Location After End of Buffer which could result in Arbitrary code execution. (CVE-2023-25865, CVE-2023-25867)
- Out-of-bounds Write which could result in Arbitrary code execution. (CVE-2023-25866)
- Use After Free which could result in Arbitrary code execution. (CVE-2023-25870, CVE-2023-25871)
- Out-of-bounds Read which could result in a Memory leak. (CVE-2023-25875, CVE-2023-25876, CVE-2023-25877, CVE-2023-25878)

Adobe Photoshop

- Use After Free which could result in Arbitrary code execution. (CVE-2023-25908)

Adobe ColdFusion

- Deserialization of Untrusted Data which could result in Arbitrary code execution. (CVE-2023-26359)
- Improper Access Control which could result in Arbitrary code execution. (CVE-2023-26360)
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'). (CVE-2023-26361)

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.
    - **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

- 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.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.

- 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.

REFERENCES:

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

https://helpx.adobe.com/security/products/magento/apsb23-17.html

https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html

https://helpx.adobe.com/security/products/illustrator/apsb23-19.html

https://helpx.adobe.com/security/products/dimension/apsb23-20.html

https://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html

https://helpx.adobe.com/security/products/substance3d_stager/apsb23-22.html

https://helpx.adobe.com/security/products/photoshop/apsb23-23.html

https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html

CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21615

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21616

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22247

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22249

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22250

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22251

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22252

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22253

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22254

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22256

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22257

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22258

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22259

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22260

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22261

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22262

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22263

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22264

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22265

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22266

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22269

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22271

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25859

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25860

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25861

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25862

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25863

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25864

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25865

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25866

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25867

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25868

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25869

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25870

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25871

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25872

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25873

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25874

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25875

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25876

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25877

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25878

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25879

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25880

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25881

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25882

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25883

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25884

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25885

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25886

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25887

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25888

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25889

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25890

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25891

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25892

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25893

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25894

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25895

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25896

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25897

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25898

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25899

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25900

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25901

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25902

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25903

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25904

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25905

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25906

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25907

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25908

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26327

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26328

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26329

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26330

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26331

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26332

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26333

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26334

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26335

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26336

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26337

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26338

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26339

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26340

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26341

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26342

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26343

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26344

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26345

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26346

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26348

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26349

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26350

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26351

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26352

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26353

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26354

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26355

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26356

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26358

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26359

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26360

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26361

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26426

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE

https://learn.cisecurity.org/e/799323/tlp/4sskqx/846687438?h=OpcxUvhLkEqlJlLZSye0sWI41mx7d5onWBsVf1pMzLw