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.

DATE(S) ISSUED:
07/12/2022

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 RoboHelp Server is a help authoring tool
- Adobe Photoshop is a graphics editor
- Adobe Acrobat and Reader are used to view, create, print, and mange PDF files
- Adobe Character and Animator is a desktop application software product that combines real-time motion-capture with a multi-track recording system to control layered 2D puppets drawn in Photoshop or Illustrator.

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 RoboHelp RH202.0.7 and earlier versions for Windows and macOS

- Adobe Acrobat DC and Adobe Acrobat Reader DC 22.001.20142 and earlier versions for Windows and macOS
- Adobe Acrobat 2020 and Acrobat Reader 2020 20.005.30334 and earlier versions for Windows
- Adobe Acrobat 2020 and Acrobat Reader 2020 20.005.30331 and earlier versions for macOS
- Adobe Acrobat 2017 and Acrobat Reader 2017 17.012.30229 and earlier versions for Windows
- Adobe Acrobat 2017 and Acrobat Reader 2017 17.012.30227 and earlier versions for macOS
- Adobe Character Animator 2021 4.4.7 and earlier versions for Windows and macOS
- Adobe Character Animator 2022 22.4 and earlier versions for Windows and macOS
- Adobe Photoshop 2021 22.5.7 and earlier versions for Windows and macOS
- Adobe Photoshop 2022 23.3.2 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

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

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

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

Adobe RoboHelp

- Cross-site Scripting, which could allow for arbitrary code execution. (CVE-2022-23201)

Adobe Photoshop

- Use After Free, which could allow for arbitrary code execution. (CVE-2022-34243)
- Access of Uninitialized Pointer, which could allow for memory leak. (CVE-2022-34244)

Adobe Acrobat and Reader

- Use After Free, which could allow for arbitrary code execution. (CVE-2022-34230, CVE-2022-34229, CVE-2022-34227, CVE-2022-34225, CVE-2022-34224, CVE-2022-34223, CVE-2022-34237, CVE-2022-34220, CVE-2022-34219, CVE-2022-34216)
- Use After Free, which could allow for memory leak. (CVE-2022-34234, CVE-2022-34233, CVE-2022-34232)
- Access of Uninitialized Pointer, which could allow for arbitrary code execution. (CVE-2022-34228)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2022-34226, CVE-2022-34222, CVE-2022-34215)
- Out-of-bounds Read, which could allow for memory leak. (CVE-2022-34238, CVE-2022-34239, CVE-2022-34236)
- Access of Resource using Incompatible Type, which could allow for arbitrary code execution. (CVE-2022-34221)
- Out-of-bounds- Write, which could allow for arbitrary code execution. (CVE-2022-34217)

Adobe Character and Animator

- Heap-based Buffer Overflow, which could allow for arbitrary code execution. (CVE-2022-34241)
- Out-of-bounds Read, which could allow for arbitrary code execution. (CVE-2022-34242).

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/robohelp/apsb22-10.html

https://helpx.adobe.com/security/products/acrobat/apsb22-32.html

https://helpx.adobe.com/security/products/character_animator/apsb22-34.html

https://helpx.adobe.com/security/products/photoshop/apsb22-35.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23201

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34215

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34216

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34217

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34219

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34220

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34221

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34222

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34223

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34224

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34225

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34226

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34227

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34228

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34229

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34230

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34232

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34233

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34234

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34236

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34237

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34238

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34239

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34241

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34242

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34243

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34244