*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:**
03/08/2022

**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.

- Illustrator is a vector graphics editor and design program.
- Photoshop is a graphics editor.
- Adobe After Effects is a digital visual effects, motion graphics, and compositing application.

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:**
- Illustrator 2022 26.0.3 and earlier versions for Windows and macOS
- Photoshop 2021 22.5.6 and earlier versions for Windows and macOS
- Photoshop 2022 23.2 and earlier versions for Windows and macOS
- Adobe After Effects 22.2 and earlier versions for Windows and macOS
- Adobe After Effects 18.4.4 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:

Adobe Illustrator

- Buffer Overflow which could allow for Arbitrary code execution (CVE-2022-23187)

Adobe Photoshop

- Access of Memory Location After End of Buffer which could allow for a Memory Leak. (CVE-2022-24090)

Adobe After Effects

- Stack-based Buffer Overflow which could allow for Arbitrary code execution. (CVE-2022-24094, CVE-2022-24095, CVE-2022-24096, CVE-2022-24097)

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.html
https://helpx.adobe.com/security/products/photoshop/apsb22-14.html
https://helpx.adobe.com/security/products/illustrator/apsb22-15.html
https://helpx.adobe.com/security/products/after_effects/apsb22-17.html

**CVE:**

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23187
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24094
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24095
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24096
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24097