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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/10/2021

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.

- Photoshop is Adobe's flagship image editing software.
- Acrobat is a family of application software and Web services mainly used to create, view and edit PDF documents.
- Illustrator is a vector graphics editor and design program.
- Animate is a multimedia authoring and computer animation program.
- Dreamweaver is used to develop and design websites.
- Magento is a leading provider of cloud commerce innovation to merchants and brands across B2C and B2B industries.

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 reports that CVE-2021-21017 has been exploited in the wild in limited attacks targeting Adobe Reader users on Windows.

SYSTEMS AFFECTED:

- Adobe Photoshop 2020 versions prior to 21.2.5
- Adobe Photoshop 2021 versions prior to 22.2
- Adobe Dreamweaver versions prior to 20.2.1 and 21.1
- Acrobat DC and Reader DC versions prior to 2021.001.20135
- Acrobat 2020 and Acrobat Reader 2020 versions prior to 2020.001.30020
- Acrobat 2017 and Acrobat Reader 2017 versions prior to 2017.011.30190
- Adobe Animate versions prior to 21.0.3
- Adobe Illustrator versions prior to 25.2
- Magento Commerce and Open Source versions prior to 2.4.2

- Magento Commerce and Open Source versions prior to 2.4.1-p1
- Magento Commerce and Open Source versions prior to 2.3.6-p1

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 Photoshop, Dreamweaver, Animate, Illustrator, Magento and Acrobat, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Adobe Photoshop

- Out-of-bounds read errors, which could allow for arbitrary code execution. (CVE-2021-21049, CVE-2021-21050)
- Out-of-bounds write error, which could allow for arbitrary code execution. (CVE-2021-21047)
- Buffer overflow vulnerabilities, which could allow for arbitrary code execution. (CVE-2021-21048, CVE-2021-21051)

Adobe Acrobat and Reader

- Buffer overflow vulnerabilities, which could allow for arbitrary code execution and denial-of-service. (CVE-2021-21046, CVE-2021-21058, CVE-2021-21059, CVE-2021-21062, CVE-2021-21063)
- Heap-based buffer overflow vulnerability, which could allow for arbitrary code execution. (CVE-2021-21017)
- Path traversal vulnerability, which could allow for arbitrary code execution. (CVE-2021-21037)
- Integer overflow vulnerability, which could allow for arbitrary code execution. (CVE-201-21036)
- Improper access control vulnerability, which could allow privilege escalation. (CVE-2021-21045)
- Out-of-bounds read errors, which could allow for privilege escalation. (CVE-2021-21042, CVE-2021-21034)
- Use-after-free vulnerabilities, which could allow for arbitrary code execution and information disclosure. (CVE-2021-21061, CVE-2021-21041, CVE-2021-21040, CVE-2021-21039, CVE-2021-21035, CVE-2021-21033, CVE-2021-21028, CVE-2021-21021)
- Out-of-bounds write errors, which could allow for arbitrary code execution. (CVE-2021-21044, CVE-2021-21038)
- NULL pointer dereference vulnerability, which could allow for information disclosure. (CVE-2021-21057)
- Improper input validation, which could allow for information disclosure. (CVE-2021-21060)

Adobe Dreamweaver

- Uncontrolled search path error, which could allow for information disclosure. (CVE-2021-21055)

Adobe Animate

- Out-of-bounds read error, which could allow for arbitrary code execution. (CVE-2021-21052)

Adobe Illustrator

- Out-of-bounds write errors, which could allow for arbitrary code execution. (CVE-2021-21053, CVE-2021-21054)

Magento

- Insecure direct object reference (IDOR) vulnerabilities, which could allow for unauthorized access to restricted resources. (CVE-2021-21012, CVE-2021-21013, CVE-2021-21022)
- File upload allow list bypass vulnerability, which could allow for arbitrary code execution. (CVE-2021-21014)
- Security bypass vulnerabilities, which could allow for arbitrary code execution. (CVE-2021-21015, CVE-2021-21016, CVE-2021-21025)
- Command injection vulnerability, which could allow for arbitrary code execution. (CVE-2021-21018)
- XML injection vulnerability, which could allow for arbitrary code execution. (CVE-2021-21019)
- Access control bypass vulnerability, which could allow for unauthorized access to restricted resources. (CVE-2021-21020)
- Stored XXS vulnerabilities, which could allow for arbitrary JavaScript execution in the browser. (CVE-2021-21023, CVE-2021-21030)
- Blind SQL injection vulnerability, which could allow for unauthorized access to restricted resources. (CVE-2021-21024)
- Improper authorization vulnerability, which could allow for unauthorized access to restricted resources. (CVE-2021-21026)
- CSRF vulnerability, which could allow for unauthorized modification of customer metadata. (CVE-2021-21027)
- Reflected XXS vulnerability, which could allow for arbitrary JavaScript execution in the browser. (CVE-2021-21029)
- Insufficient invalidation of user session vulnerabilities, which could allow for unauthorized access to restricted resources. (CVE-2021-21031, CVE-2021-21032)

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/products/dreamweaver/apsb21-13.html
https://helpx.adobe.com/security/products/illustrator/apsb21-12.html
https://helpx.adobe.com/security/products/animate/apsb21-11.html
https://helpx.adobe.com/security/products/photoshop/apsb21-10.html
https://helpx.adobe.com/security/products/magento/apsb21-08.html
https://helpx.adobe.com/security/products/acrobat/apsb21-09.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21036
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21045
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21048

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21050
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21051
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21058
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21060
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-21063

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/