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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
08/10/2021

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.

- Connect is a suite of software for remote training, web conferencing, presentation, and desktop sharing.
- 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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Adobe Connect versions prior to 11.2.3
- Magento Commerce and Open Source versions prior to 2.4.3
- Magento Commerce and Open Source versions prior to 2.4.2-p2
- Magento Commerce and Open Source versions prior to 2.3.1-p1

RISK:
Government:
- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **Medium**
- 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 Connect

- Violation of Secure Design Principles, which could allow for security feature bypass (CVE-2021-36061)
- Reflected Cross-site Scripting, which could allow for arbitrary code execution. (CVE-2021-36062, CVE-2021-36063)

Adobe Magento Commerce and Open Source

- Business Logic Error, which could allow for security feature bypass. (CVE-2021-36012)
- Stored Cross-site Scripting, which could allow for arbitrary code execution. (CVE-2021-36026, CVE-2021-36027)
- Improper Access Control, which could allow for arbitrary code execution. (CVE-2021-36036)
- Improper Authorization, which could allow for security feature bypass. (CVE-2021-36029, CVE-2021-36037)
- Improper Input Validation, which could allow for application denial of service. (CVE-2021-36044)
- Improper Input Validation, which could allow for privilege escalation. (CVE-2021-36032)
- Improper Input Validation, which could allow for security feature bypass. (CVE-2021-36030, CVE-2021-36038)
- Improper Input Validation, which could allow for arbitrary code execution. (CVE-2021-36021, CVE-2021-36024, CVE-2021-36025, CVE-2021-36034, CVE-2021-36035, CVE-2021-36040, CVE-2021-36041, CVE-2021-36042)
- Path Traversal, which could allow for arbitrary code execution. (CVE-2021-36031)
- OS Command Injection, which could allow for arbitrary code execution. (CVE-2021-36022, CVE-2021-36023)
- Incorrect Authorization, which could allow for arbitrary file system. (CVE-2021-36039)
- Server-Side Request Forgery, which could allow for arbitrary code execution. (CVE-2021-36043)
- XML Injection, which could allow for arbitrary code execution. (CVE-2021-36020, CVE-2021-36028, CVE-2021-36033)

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/magento/apsb21-64.html
https://helpx.adobe.com/security/products/connect/apsb21-66.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36036
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36063