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:
02/18/2022

SUBJECT:
Multiple Vulnerabilities in Adobe Commerce and Magento Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Commerce and Magento Open Source, the most severe of which could allow for remote code execution.

- Adobe Commerce is a leading provider of cloud commerce innovation to merchants and brands across B2C and B2B industries.
- Magento is a web-based e-commerce application written in PHP.

Successful exploitation of the most severe of these vulnerabilities could allow for remote 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:
Adobe is aware that CVE-2022-24086 has been exploited in the wild in very limited attacks targeting Adobe Commerce merchants.

SYSTEMS AFFECTED:
- Adobe Commerce 2.4.3-p1 and earlier versions
- Adobe Commerce 2.3.7-p2 and earlier versions
- Magento Open Source 2.4.3-p1 and earlier versions
- Magento Open Source 2.3.7-p2 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 Commerce and Magento Open Source, the most severe of which could allow for remote code execution.

- Improper input validation vulnerability, which could for remote code execution. (CVE-2022-24086 & CVE-2022-24087)

Successful exploitation of the most severe of these vulnerabilities could allow for remote 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/security-bulletin.html

https://helpx.adobe.com/security/products/magento/apsb22-12.html

TheHackerNews:

https://thehackernews.com/2022/02/critical-magento-0-day-vulnerability.html

https://thehackernews.com/2022/02/another-critical-rce-discovered-in.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24086

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24087