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:
04/10/2019

SUBJECT:
Multiple Vulnerabilities in Adobe Shockwave Player Could Allow for Arbitrary Code Execution (APSB19-20)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Shockwave Player, which could allow for arbitrary code execution. Adobe Shockwave Player was a multimedia platform for building browser-based, interactive applications and video games. It has reached its end of life as of April 9th, 2019 and is no longer supported for users without an enterprise license. Successful exploitation of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There have been no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Adobe Shockwave Player for Windows version 12.3.4.204 and earlier

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 Shockwave Player, which could allow for arbitrary code execution. The details of these vulnerabilities are as follows:

- Seven memory corruption vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7098, CVE-2019-7099, CVE-2019-7100, CVE-2019-7101, CVE-2019-7102, CVE-2019-7103, CVE-2019-7104)

Successful exploitation of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Adobe customers with enterprise licenses will continue to receive product support. Consult your support representative to identify whether a patch is available to you.
- For all users, it is recommended to identify and migrate to a supported, alternative solution.
- Remove Shockwave player from any systems that do not have a critical business need for it.
- For business critical applications that cannot be patched due to lack of an enterprise license, enable heightened monitoring such as network and host intrusion detection systems, and exploit mitigation tools such as Windows Defender Exploit Guard.
- Enable read-only protected view for Microsoft Office.
- 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 websites or follow links provided by unknown or untrusted 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/shockwave/apsb19-20.html
https://helpx.adobe.com/shockwave/shockwave-end-of-life-faq.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7098
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7099
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7100
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7101
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7102
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7103
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7104