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:
04/09/2019

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Arbitrary Code Execution (APSB19-19)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for arbitrary code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe 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 Flash Player Desktop Runtime for Windows, macOS and Linux version 32.0.0.156 and earlier
- Adobe Flash Player for Google Chrome for Windows, macOS, Linux and Chrome OS version 32.0.0.156 and earlier
- Adobe Flash Player for Microsoft Edge and Internet Explorer for Windows 10 and 8. Version 111 32.0.0.156 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 Flash Player, the most severe of which could allow for arbitrary code execution. The details of these vulnerabilities are as follows:

- An Out-of-bounds read vulnerability that could allow for Information Disclosure. (CVE-2019-7108)
- A Use After Free vulnerability that could allow for Arbitrary Code Execution. (CVE-2019-7096)

Successful exploitation of the most severe 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:

- Apply the update provided by Adobe to vulnerable systems immediately after appropriate testing.
- Enable click-to-play to require user interaction before enabling SWF content for Internet Explorer 7 and below.
- 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/flash-player/apsb19-19.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7096
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7108