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 Acrobat and Reader Could Allow for Arbitrary Code Execution (APSB19-17)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. Adobe Acrobat and Reader allow a user to view, create, manipulate, print and manage files in Portable Document Format (PDF). 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 the user, 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 the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

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

SYSTEMS AFFECTED:
- Acrobat DC (Continuous track) for Windows and macOS version 2019.010.20098 and earlier versions
- Acrobat Reader DC (Continuous Track) for Windows and macOS version 2019.010.20098 and earlier versions
- Acrobat 2017 (Classic 2017 Track) for Windows and macOS version 2017.011.30127 and earlier version
- Acrobat Reader 2017 (Classic 2017 Track) for Windows and macOS version 2017.011.30127 and earlier version
- Acrobat DC (Classic 2015 Track) for Windows and macOS version 2015.006.30482 and earlier versions
- Acrobat Reader DC (Classic 2015 Track) for Windows and macOS version 2015.006.30482 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 Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. The vulnerabilities are as follows:

- Multiple Out-of-Bounds Read vulnerabilities that could allow for Information Disclosure. (CVE-2019-7061, CVE-2019-7109, CVE-2019-7110, CVE-2019-7114, CVE-2019-7115, CVE-2019-7116, CVE-2019-7121, CVE-2019-7122, CVE-2019-7123, CVE-2019-7127)
- Multiple Out-of-Bounds Write vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7111, CVE-2019-7118, CVE-2019-7119, CVE-2019-7120, CVE-2019-7124)
- Multiple Type Confusion vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7117, CVE-2019-7128)
- Multiple Use After Free vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7088, CVE-2019-7112)
- Multiple Heap Overflow vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7113, CVE-2019-7125)

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 the user, 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 the most severe of these vulnerabilities could have less impact than if it was configured with administrative 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 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:

https://helpx.adobe.com/security/products/acrobat/apsb19-17.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7061
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7088
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7109
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7110
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7111
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7112

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7113
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7114
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7115
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7116
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7117
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7118
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7120
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7121
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7122
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7123
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7124
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7125
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7127
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7128