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:
05/14/2019

SUBJECT:
Multiple Vulnerabilities in Adobe Acrobat and Reader Could Allow for Arbitrary Code Execution (APSB19-18)

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 2019.010.20100 and earlier versions
- Acrobat Reader DC (Continuous Track) for Windows and macOS version 2019.010.20099 and earlier versions
- Acrobat 2017 (Classic 2017 Track) for Windows and macOS version 2017.011.30140 and earlier version
- Acrobat Reader 2017 (Classic 2017 Track) for Windows and macOS version 2017.011.30138 and earlier version
- Acrobat DC (Classic 2015 Track) for Windows and macOS version 2015.006.30495 and earlier versions
- Acrobat Reader DC (Classic 2015 Track) for Windows and macOS version 2015.006.30493 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. Details of these vulnerabilities are as follows:

- Multiple Out-of-Bounds Read vulnerabilities that could allow for Information Disclosure. (CVE-2019-7841, CVE-2019-7836, CVE-2019-7826, CVE-2019-7819, CVE-2019-7813, CVE-2019-7812, CVE-2019-7811, CVE-2019-7810, CVE-2019-7803, CVE-2019-7802, CVE-2019-7801, CVE-2019-7799, CVE-2019-7798, CVE-2019-7795, CVE-2019-7794, CVE-2019-7793, CVE-2019-7790, CVE-2019-7789, CVE-2019-7787, CVE-2019-7780, CVE-2019-7778, CVE-2019-7777, CVE-2019-7776, CVE-2019-7775, CVE-2019-7774, CVE-2019-7773, CVE-2019-7771, CVE-2019-7770, CVE-2019-7769, CVE-2019-7758, CVE-2019-7145, CVE-2019-7144, CVE-2019-7143, CVE-2019-7142, CVE-2019-7141, CVE-2019-7140)
- Multiple Out-of-Bounds Write vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7829, CVE-2019-7825, CVE-2019-7822, CVE-2019-7818, CVE-2019-7804, CVE-2019-7800)
- A Type Confusion vulnerability that could allow for Arbitrary Code Execution. (CVE-2019-7820)
- Multiple Use After Free vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7835, CVE-2019-7834, CVE-2019-7833, CVE-2019-7832, CVE-2019-7831, CVE-2019-7830, CVE-2019-7823, CVE-2019-7821, CVE-2019-7817, CVE-2019-7814, CVE-2019-7809, CVE-2019-7808, CVE-2019-7807, CVE-2019-7806, CVE-2019-7805, CVE-2019-7797, CVE-2019-7796, CVE-2019-7792, CVE-2019-7791, CVE-2019-7788, CVE-2019-7786, CVE-2019-7785, CVE-2019-7783, CVE-2019-7782, CVE-2019-7781, CVE-2019-7772, CVE-2019-7768, CVE-2019-7767, CVE-2019-7766, CVE-2019-7765, CVE-2019-7764, CVE-2019-7763, CVE-2019-7762, CVE-2019-7761, CVE-2019-7760, CVE-2019-7759)
- Multiple Heap Overflow vulnerabilities that could allow for Arbitrary Code Execution. (CVE-2019-7828, CVE-2019-7827)
- A Buffer Error vulnerability that could allow for Arbitrary Code Execution. (CVE-2019-7824)
- A Double Free vulnerability that could allow for Arbitrary Code Execution. (CVE-2019-7784)
- A Security Bypass vulnerability that could allow for Arbitrary Code Execution. (CVE-2019-7779)

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/apsb19-18.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7140
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7141
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7142
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7143
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7144
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7145
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7758
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7759
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7760
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7762
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7763
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7764
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7765
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7766
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7767
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7768
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7769
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7770
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7771
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7772
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7773
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7774
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7775
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7776
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7777
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7778
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7779
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7780
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7781
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7782
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7783
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7784
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7785
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7786
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7787
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7788
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7789
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7790

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7791
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7792
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7793
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7794
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7795
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7796
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7797
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7798
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7799
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7800
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7801
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7802
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7803
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7804
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7806
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7808
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7809
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7810
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7811
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7812
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7813
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7814
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7820
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7823
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7824
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7825
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7826
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7827
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7828
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7829
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7831
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7832
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7833
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7834
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7835
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7836
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7841

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov