

*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:**

08/13/2019

**SUBJECT:**

Multiple Vulnerabilities in Adobe Acrobat and Reader Could Allow for Arbitrary Code Execution (APSB19-41)

**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 version 2019.012.20035 and prior
- Acrobat DC (Continuous Track) for macOS version 2019.012.20034 and prior
- Acrobat Reader DC (Continuous Track) for Windows version 2019.012.20035 and prior
- Acrobat Reader DC (Continuous Track) for macOS version 2019.012.20034 and prior
- Acrobat DC (Classic 2017 Track) for Windows version 2017.011.30143 and prior
- Acrobat DC (Classic 2017 Track) for macOS version 2017.011.30142 and prior
- Acrobat Reader DC (Classic 2017 Track) for Windows version 2017.011.30143 and prior
- Acrobat Reader DC (Classic 2017 Track) for macOS version 2017.011.30142 and prior
- Acrobat DC (Classic 2015 Track) for Windows version 2015.006.30497 and prior
- Acrobat DC (Classic 2015 Track) for macOS version 2015.006.30498 and prior
- Acrobat Reader DC (Classic 2015 Track) for Windows version 2015.006.30498 and prior
- Acrobat Reader DC (Classic 2015 Track) for macOS version 2015.006.30497 and prior

**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-2019-8077, CVE-2019-8094, CVE-2019-8095, CVE-2019-8096, CVE-2019-8102, CVE-2019-8103, CVE-2019-8104, CVE-2019-8105, CVE-2019-8106, CVE-2019-8002, CVE-2019-8004, CVE-2019-8005, CVE-2019-8007, CVE-2019-8010, CVE-2019-8011, CVE-2019-8012, CVE-2019-8018, CVE-2019-8020, CVE-2019-8021, CVE-2019-8032, CVE-2019-8035, CVE-2019-8037, CVE-2019-8040, CVE-2019-8043, CVE-2019-8052)
- Multiple out-of-bounds write vulnerabilities that could allow for arbitrary code execution (CVE-2019-8098, CVE-2019-8100, CVE-2019-7965, CVE-2019-8008, CVE-2019-8009, CVE-2019-8016, CVE-2019-8022, CVE-2019-8023, CVE-2019-8027)
- A command injection vulnerability that could allow for arbitrary code execution (CVE-2019-8060)
- Multiple use after free vulnerabilities that could allow for arbitrary code execution (CVE-2019-8003, CVE-2019-8013, CVE-2019-8024, CVE-2019-8025, CVE-2019-8026, CVE-2019-8028, CVE-2019-8029, CVE-2019-8030, CVE-2019-8031, CVE-2019-8033, CVE-2019-8034, CVE-2019-8036, CVE-2019-8038, CVE-2019-8039, CVE-2019-8047, CVE-2019-8051, CVE-2019-8053, CVE-2019-8054, CVE-2019-8055, CVE-2019-8056, CVE-2019-8057, CVE-2019-8058, CVE-2019-8059, CVE-2019-8061)
- Multiple heap overflow vulnerabilities that could allow for privilege escalation (CVE-2019-7832, CVE-2019-8014, CVE-2019-8015, CVE-2019-8041, CVE-2019-8042, CVE-2019-8046, CVE-2019-8049, CVE-2019-8050)
- A buffer error vulnerability that could lead to arbitrary code execution (CVE-2019-8048)
- A double free vulnerability that could allow for arbitrary code execution (CVE-2019-8044)
- Multiple integer overflow vulnerabilities that could allow for information disclosure (CVE-2019-8099, CVE-2019-8101)
- A type confusion vulnerability could allow for arbitrary code execution (CVE-2019-8019)
- Multiple untrusted pointer dereference vulnerabilities that could allow for arbitrary code execution (CVE-2019-8006, CVE-2019-8017, CVE-2019-8045)

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/apsb19-41.html>

## CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7832>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7965>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8002>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8003>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8004>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8005>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8006>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8007>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8008>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8009>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8010>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8011>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8012>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8013>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8014>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8015>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8016>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8017>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8018>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8019>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8020>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8021>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8022>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8023>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8024>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8025>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8026>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8027>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8028>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8029>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8030>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8031>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8032>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8033>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8034>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8035>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8036>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8037>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8038>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8039>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8040>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8041>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8042>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8043>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8044>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8045>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8046>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8047>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8048>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8049>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8050>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8051>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8052>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8053>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8054>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8055>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8056>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8057>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8058>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8059>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8060>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8061>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8077>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8094>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8095>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8096>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8097>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8098>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8099>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8100>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8101>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8102>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8103>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8104>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8105>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8106>

**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/>