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 Photoshop CC Could Allow for Arbitrary Code Execution (APSB19-44)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Photoshop CC, the most severe of which could allow for arbitrary code execution. Adobe Photoshop CC is a graphics editor program. Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. 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 are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Photoshop CC 19.1.8 and earlier
- Photoshop CC 20.0.5 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 Photoshop CC which could allow for arbitrary code execution. Details of these vulnerabilities are included below:

- Multiple heap corruption vulnerabilities that could allow for arbitrary code execution (CVE-2019-7978, CVE-2019-7980, CVE-2019-7985, CVE-2019-7990, CVE-2019-7993)
- Multiple type confusion vulnerabilities that could allow for arbitrary code execution (CVE-2019-7969, CVE-2019-7970, CVE-2019-7971, CVE-2019-7972, CVE-2019-7973, CVE-2019-7974, CVE-2019-7975)
- Multiple out of bound read vulnerabilities that could lead to memory leakage (CVE-2019-7977, CVE-2019-7981, CVE-2019-7987, CVE-2019-7991, CVE-2019-7992, CVE-2019-7995, CVE-2019-7996, CVE-2019-7997, CVE-2019-7998, CVE-2019-7999, CVE-2019-8000, CVE-2019-8001)
- Multiple command injection vulnerabilities that could allow for arbitrary code execution (CVE-2019-7968, CVE-2019-7989)
- Multiple out of bound write vulnerabilities that could allow for arbitrary code execution (CVE-2019-7976, CVE-2019-7979, CVE-2019-7982, CVE-2019-7983, CVE-2019-7984, CVE-2019-7986, CVE-2019-7988, CVE-2019-7994)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. 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:

- 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:
Adobe:
https://helpx.adobe.com/security/products/photoshop/apsb19-44.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7979

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7994
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7996
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7997
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8000
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8001