

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:

01/12/2021

SUBJECT:

A Vulnerability in Adobe Photoshop Could Allow for Arbitrary Code Execution (APSB21-01)

OVERVIEW:

A vulnerability has been discovered in Adobe Photoshop which could allow for arbitrary code execution. Photoshop is Adobe's flagship image editing software. Successful exploitation of this vulnerability could allow for arbitrary code execution. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Adobe Photoshop 2021 versions prior to 22.1

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:

A buffer overflow vulnerability has been discovered in Adobe Photoshop which could allow an attacker to execute arbitrary code in the context of the application. This vulnerability is caused by a failure to perform a bounds check on input. The attack would occur via an unsuspecting user opening a malicious file with the vulnerable program.

Successful exploitation of this vulnerability could allow for arbitrary code execution. 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. Users whose accounts are

configured to have fewer user rights on the system could be less impacted than those who operate with administrative user 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 un-trusted websites or follow links provided by unknown or un-trusted 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/apsb21-01.html>

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/>