

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:

07/21/2020

SUBJECT:

Multiple Vulnerabilities in Adobe Bridge Could Allow for Arbitrary Code Execution (APSB20-44)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Bridge that could allow for arbitrary code execution. Adobe Bridge is a file management application that manages files across multiple Adobe programs. Successful exploitation of these vulnerabilities could result in arbitrary code execution within the context of the application and an attacker gaining the same privileges as the logged-on user. 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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Adobe Bridge versions prior to 10.0.3

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 Bridge that could allow for arbitrary code execution. The vulnerabilities are as follows:

- Out-of-bounds read vulnerability that could allow for arbitrary code execution (CVE-2020-9675)

- Out-of-bounds write vulnerabilities that could allow for arbitrary code execution (CVE-2020-9674, CVE-2020-9676)

Successful exploitation of these vulnerabilities could result in arbitrary code execution within the context of the application and an attacker gaining the same privileges as the logged-on user. 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 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/bridge/apsb20-44.html>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9675>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9674>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9676>

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/>