

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

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

06/17/2015

SUBJECT:

Multiple Vulnerabilities in Adobe Products Could Allow Remote Code Execution (APSB15-12) (APSB15-13)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Photoshop Creative Cloud and Adobe Bridge Creative Cloud. Adobe Photoshop CC is a cloud based image and design application that allows users to edit images and create graphics. Adobe Bridge Creative Cloud is a cloud based file management application that manages files across multiple Adobe programs.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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 users who operate with administrative user rights.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Bridge CC 6.1 and earlier versions
- Adobe Photoshop CC 2015 16.0 and earlier versions

RISK:

Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Medium

TECHNICAL SUMMARY:

Multiple Adobe products are prone to multiple vulnerabilities. These vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2015-3109, CVE-2015-3112).
- Integer overflow vulnerability that could lead to code execution (CVE-2015-3110).
- Heap overflow vulnerability that could lead to code execution (CVE-2015-3111)

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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 users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to those required only.

REFERENCES:

Adobe:

<https://helpx.adobe.com/security/products/photoshop/apsb15-12.html>
<https://helpx.adobe.com/security/products/bridge/apsb15-13.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3109>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3110>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3111>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3112>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>