

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:

3/10/2015

SUBJECT:

Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (MS15-021)

OVERVIEW:

Multiple vulnerabilities in Adobe Font Driver could allow remote code execution. Adobe Font Driver allows Windows systems to display a range of fonts to enhance the user experience when visiting web pages or reading documents or email messages. Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE

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

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1
- Server core

RISK:

Government:

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

Businesses:

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

Home users: High

TECHNICAL SUMMARY:

Adobe Font Driver is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

- A denial of service vulnerability due to how the Adobe Font Driver manages memory when parsing fonts. (CVE-2015-0074).
- Multiple information disclosure vulnerabilities that could allow the disclosure of memory contents to an attacker. (CVE-2015-0087, CVE-2015-0089).

- Multiple remote code execution vulnerabilities due to the Adobe Font Driver improperly overwriting objects in memory. (CVE-2015-0088, CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, CVE-2015-0093).

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit 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:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms15-021.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0074>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0087>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0088>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0089>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0090>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0091>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0092>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0093>

TLP: WHITE

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

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