

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:

08/11/2015

SUBJECT:

Vulnerabilities in Microsoft Office Graphics Component Could Allow Remote Code Execution (MS15-080)

OVERVIEW:

Multiple vulnerabilities have been discovered in the Microsoft Office graphics component that could allow for remote code execution. Successful exploitation of these vulnerabilities could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker may exploit these vulnerabilities by redirecting users to a specially crafted webpage or by users opening a specially crafted document.

THREAT INTELLIGENCE

Microsoft reports that CVE-2015-2433 has been publicly disclosed.

SYSTEM AFFECTED:

- Windows Server 2008 including R2
- Windows Server 2012 including R2
- Windows Server Core
- Windows RT
- Windows RT 8.1
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Microsoft Office 2007 – Service Pack 3
- Microsoft Office 2010 – Service Pack 2
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010
- Microsoft Lync 2010 Attendee
- Microsoft Lync 2013
- Microsoft Silverlight 5

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:

Multiple vulnerabilities have been discovered in Microsoft Office graphics component that could allow for remote code execution. These vulnerabilities are described below:

- Six OpenType Font Parsing vulnerabilities exist which could give an attacker complete control of the affected system (CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462).
- Five TrueType Font Parsing vulnerabilities exist which could give an attacker complete control of the affected system (CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463, CVE-2015-2464).
- One vulnerability in Microsoft Office Graphics Component exists which could allow an attacker to execute remote code (CVE-2015-2431).

Successful exploitation of these vulnerabilities could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker may exploit these vulnerabilities by redirecting users to a specially crafted webpage or by users opening a specially crafted document.

The Microsoft bulletin also patches the following unrelated vulnerabilities:

- One Kernel Address Space Layout Randomization (ASLR) Bypass vulnerability exists which could allow an attacker to retrieve information about ASLR and bypass it (CVE-2015-2433).
- One Windows Client/Server Run-time Subsystem (CSRSS) Elevation of Privilege vulnerability exists which could lead to disclosure of sensitive information (CVE-2015-2453).
- One Windows kernel-mode driver (KMD) Security Feature Bypass vulnerability exists which could allow an attacker to gain elevated privileges on the affected system (CVE-2015-2454).
- One Windows Shell Security Feature Bypass vulnerability exists which could allow an attacker to gain elevated privileges on the affected system (CVE-2015-2465).

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems 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 those from un-trusted sources.
- Workaround options are also available via the Microsoft link listed in the reference section

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS15-080>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2431>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2432>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2433>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2435>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2453>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2454>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2455>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2456>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2458>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2459>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2460>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2461>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2462>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2463>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2464>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2465>

TLP: WHITE

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

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