

*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 Could Allow Remote Code Execution (MS15-081)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers 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:**

A memory corruption vulnerability, CVE-2015-1642 is currently being exploited in the wild.

**SYSTEM AFFECTED:**

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT
- Microsoft Office for Mac 2011
- Microsoft Office for Mac 2016
- Microsoft Office Compatibility Pack
- Microsoft Word Viewer
- Microsoft Automation Services on Microsoft SharePoint Server 2010
- Microsoft Automation Services on Microsoft SharePoint Server 2013
- Microsoft Word Web Apps 2010
- Microsoft Office Web Apps Server 2013

**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:**

Eight vulnerabilities have been reported in Microsoft Office, one of which has been publicly disclosed. Seven of these vulnerabilities can be triggered by opening a specially crafted file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted file as an email attachment. In the web based scenario, a user would have to open the specially crafted file that is hosted on a website. When the user opens the file, the attacker's supplied code will execute.

The eighth vulnerability requires an attacker to leverage a separate vulnerability and execute code in Internet Explorer.

- Five remote code execution vulnerabilities exist in the way Office handles objects in memory (CVE-2015-1642, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2477).
- A remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly validate templates (CVE-2015-2466).
- A remote code execution vulnerability exists when Office decreases an integer value beyond its intended minimum value (CVE-2015-2470).
- An information disclosure vulnerability exists in Microsoft Windows, Internet Explorer, and Microsoft Office when files at a medium integrity level become accessible to Internet Explorer running in Enhanced Protection Mode (EPM). To exploit this vulnerability, an attacker would first need to leverage another vulnerability and execute code in Internet Explorer with EPM, and then execute Excel, Notepad, PowerPoint, Visio, or Word using an unsafe command line parameter. (CVE-2015-2423) This vulnerability has been publicly disclosed.

#### **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 from un-trusted sources.

#### **REFERENCES:**

##### **Microsoft:**

<https://technet.microsoft.com/library/security/MS15-081>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1642>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2423>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2466>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2467>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2468>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2469>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2470>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2477>

#### **TLP: WHITE**

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

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