

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:

07/14/2015

SUBJECT:

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-070)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office that could allow remote code execution. Successful exploitation of these vulnerabilities could result in 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.

THREAT INTELLIGENCE

There are reports of CVE-2015-2424 being exploited in the wild.

SYSTEM AFFECTED:

- Microsoft Excel 2007, Microsoft PowerPoint 2007, Microsoft Word 2007
- Microsoft Office 2010, Microsoft Excel 2010, Microsoft PowerPoint 2010, Microsoft Word 2010
- Microsoft Excel 2013, Microsoft PowerPoint 2013, Microsoft Word 2013
- Microsoft Excel 2013 RT, Microsoft PowerPoint 2013 RT, Microsoft Word 2013 RT
- Microsoft Excel for Mac 2011
- Microsoft Excel Viewer, Microsoft Office Compatibility Pack, Microsoft Word Viewer
- Excel Services on Microsoft SharePoint Server 2007
- Excel Services on Microsoft SharePoint Server 2010
- Excel Services on Microsoft SharePoint 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:**

Multiple remote code execution vulnerabilities exist in Microsoft Office software when the Office software fails to properly handle objects in memory. Exploitation of these vulnerabilities requires that a user open a specially crafted file with an affected version of Microsoft Office software.

Successful exploitation could result in 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 users who operate with administrative user rights.

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.

REFERENCES:**Adobe:**

<https://technet.microsoft.com/en-us/library/security/MS15-070>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2376>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2377>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2379>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2380>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2415>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2424>

TLP: WHITE

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

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