

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:

09/08/2015

SUBJECT:

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-099)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office which 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-2015-2545 being exploited in limited targeted attacks.

SYSTEM AFFECTED:

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT
- Microsoft Excel for Mac 2011
- Microsoft Excel for Mac 2016
- Microsoft SharePoint Foundation 2013
- 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:

Five vulnerabilities have been reported in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file and can be exploited via email or web. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Users whose accounts

are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Details of these vulnerabilities are as follows:

- Three memory corruption vulnerabilities exist in the way Office handles objects in memory (CVE-2015-2520, CVE-2015-2521, CVE-2015-2523).
- One Malformed EPS File Vulnerability (CVE-2015-2545). This vulnerability is being publicly exploited in limited targeted attacks.
- One Microsoft SharePoint XSS Spoofing Vulnerability (CVE-2015-2522).

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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- If patching is not possible immediately multiple workarounds are listed in the Microsoft reference below
- 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/MS15-099>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2520>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2521>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2522>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2523>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2545>

TLP: WHITE

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

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