

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:

01/12/2016

SUBJECT:

Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS16-004)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office that could allow remote code execution. These vulnerabilities can be exploited when a user opens a specially crafted email or office file. 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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Office 2007, 2010, 2013, 2016
- Microsoft Office 2013 RT
- Microsoft Office for Mac 2011 and Office 2016 for Mac
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft Excel Viewer
- Microsoft Word Viewer
- Microsoft SharePoint Server 2013 and Foundation 2013
- Microsoft Visual Basic 6.0 Runtime

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 discovered in Microsoft Office, the most severe of which could allow for remote code execution if a user opens a specially crafted Microsoft Office file. Details of these vulnerabilities are as follows:

- Two memory corruption vulnerabilities exist in the way Microsoft Office handles objects in memory (CVE-2016-0010, CVE-2016-0035)
- Two security bypass vulnerabilities exist in Microsoft SharePoint (CVE-2016-0011, CVE-2015-6117)
- One ASLR bypass vulnerability exists in Microsoft Office (CVE-2016-0012)

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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Apply appropriate patches provided by Microsoft for Mac vulnerable systems when patches become available.
- 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 untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS16-004>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0010>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0011>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0012>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6117>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0035>

TLP: WHITE

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

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