

*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:**

04/21/2016

**SUBJECT:**

Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution (MS16-042)

**EXECUTIVE SUMMARY:**

Multiple 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. 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.

**SOFTWARE AFFECTED:**

- Microsoft Office 2007, 2010, 2013, 2013 RT, 2016
- Microsoft Office Mac 2011 and 2016 for Mac
- Microsoft SharePoint Server 2010, 2013
- Microsoft Office Web Apps 2010, 2013

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities exist in Microsoft Office, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Four remote code execution vulnerabilities exist in Microsoft Office software when the Office software fails to properly handle objects in memory. Note that the Preview Pane is an attack vector for CVE-2016-0127. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. (CVE-2016-0122, CVE-2016-0127, CVE-2016-0136, CVE-2016-0139)

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. 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.

#### **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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

#### **REFERENCES:**

##### **Microsoft:**

<https://technet.microsoft.com/library/security/MS16-042>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0122>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0127>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0136>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0139>

#### **TLP: WHITE**

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

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