

*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:**

05/12/2015

**SUBJECT:**

Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS15-046)

**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 no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office for Mac 2011
- Microsoft PowerPoint Viewer
- Microsoft Office Web Apps 2010
- Microsoft Office Web Apps Server 2013
- Microsoft SharePoint Server 2010
- Microsoft SharePoint Server 2013
- Microsoft SharePoint Foundation 2010

**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 vulnerabilities have been discovered in Microsoft Office which could allow for remote code execution due to the way Microsoft Office parses specially crafted Microsoft Office files. These vulnerabilities could be exploited by convincing an unsuspecting user to open a specially crafted e-mail attachment or click a malicious link to an untrusted website.

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:**

### **Microsoft:**

<https://technet.microsoft.com/library/security/MS15-046>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1682>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1683>

### **TLP: WHITE**

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

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