

*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.*

**DATE(S) ISSUED:**

04/08/2014

**SUBJECT:**

Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (MS14-017)

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in Microsoft Office which could allow an attacker to take complete control of an affected system. 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.

**SYSTEM AFFECTED:**

- Microsoft Office 2003 SP3
- Microsoft Office 2007 SP3
- Microsoft Office 2010 32-bit SP1 and SP2
- Microsoft Office 2010 64-bit SP1 and SP2
- Microsoft Office 2013 32 bit
- Microsoft Office 2013 64-bit

**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:**

One memory corruption vulnerability that could allow for remote code execution has been publicly disclosed and has been reported to be activity exploited in the wild. CIS released advisory 2014-027 on

3/24/14 with information detailing this vulnerability. Additionally, one file format converter vulnerability and one stack overflow vulnerability have been privately reported to Microsoft that could allow for remote code execution. The vulnerabilities are caused when Microsoft Word does not properly handle objects in memory while parsing specially crafted Office files. These vulnerabilities can be triggered by opening a specially crafted file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted file as an email attachment. In the web based scenario, a user would have to open the specially crafted file that is hosted on a website. As long as the user opens the file using Microsoft Office, the attacker's supplied code will execute.

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.

## **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 from un-trusted sources.

## **REFERENCES:**

### **Microsoft:**

<https://technet.microsoft.com/en-us/security/bulletin/ms14-017>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1757>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1758>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1761>

### **CIS:**

<http://msisac.cisecurity.org/advisories/2014/2014-027.cfm>