

*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:**

03/24/2014

04/08/2014 - **Updated**

**SUBJECT:**

Memory Corruption Vulnerability in Microsoft Word Could Allow Remote Code Execution

**EXECUTIVE SUMMARY:**

A memory corruption vulnerability has been discovered in Microsoft Word that could allow for remote code execution. An attacker can exploit this issue to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

**April 8, 2014 UPDATED EXECUTIVE SUMMARY:**

***Microsoft has issued a patch for this vulnerability and included it in security bulletin MS14-017.***

**THREAT INTELLIGENCE**

According to a post on Microsoft Security Research and Defense Blog, this vulnerability is actively being exploited in targeted attacks directed at Microsoft Word 2010. These targeted attacks take advantage of the RTF parsing vulnerability and an Address Space Layout Randomization (ASLR) bypass which depends on a module loaded at a predictable memory address. The blog posting mentions that the Enhanced Mitigation Experience Toolkit (EMET) default configuration was tested against this attack and was found to effectively stop the exploit attempt. Please see <http://blogs.technet.com/b/srd/archive/2014/03/24/security-advisory-2953095-recommendation-to-stay-protected-and-for-detections.aspx> for the rest of the blog posting.

**SYSTEM AFFECTED:**

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office Compatibility Pack SP3

**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:**

A memory corruption vulnerability has been discovered in Microsoft Word that could allow for remote code execution. Specifically, this issue occurs when Microsoft Word parses a specially crafted Rich Text Format (RTF) file. To exploit this issue, an attacker would need to entice an unsuspecting user to view the specially crafted RTF file. Successful exploitation of this vulnerability will allow attackers to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

**RECOMMENDATIONS:**

The following actions should be taken:

- Microsoft has released a security advisory regarding this vulnerability and has provided a "Fix it" solution which makes it impossible for Microsoft Word to open RTF files. This will prevent the exploitation of this vulnerability. See <http://technet.microsoft.com/en-us/security/advisory/2953095> for more information about this solution.
- 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.

**April 8, 2014 UPDATED RECOMMENDATIONS:**

- ***Install the updates provided by Microsoft immediately after appropriate testing.***

**REFERENCES:****Microsoft:**

<http://technet.microsoft.com/en-us/security/advisory/2953095>

<http://blogs.technet.com/b/srd/archive/2014/03/24/security-advisory-2953095-recommendation-to-stay-protected-and-for-detections.aspx>

<http://technet.microsoft.com/en-us/security/jj653751> - Enhanced Mitigation Experience Toolkit (EMET)

**Security Focus:**

<http://www.securityfocus.com/bid/66385>

**CVE:**

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

**April 8, 2014 *UPDATED REFERENCES:***

**Microsoft:**

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