

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

SUBJECT:

Vulnerability in Microsoft Word Could Allow Remote Code Execution (2953095)

OVERVIEW:

A vulnerability has been discovered in Microsoft Word that could result in remote code execution. Exploitation may occur if a user opens a specially crafted RTF file using an affected version of Microsoft Word, or previews or opens a specially crafted RTF email message in Microsoft Outlook while using Microsoft Word as the email viewer.

Successful exploitation of this vulnerability could result in the attacker gaining the same rights 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.

SYSTEMS AFFECTED:

- Microsoft Word 2003 Service Pack 3
- Microsoft Word 2007 Service Pack 3
- Microsoft Word 2010 Service Pack 1 (32-bit editions)
- Microsoft Word 2010 Service Pack 2 (32-bit editions)
- Microsoft Word 2010 Service Pack 1 (64-bit editions)
- Microsoft Word 2010 Service Pack 2 (64-bit editions)
- Microsoft Word 2013 (32-bit editions)
- Microsoft Word 2013 (64-bit editions)

- Microsoft Word 2013 RT
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft Office for Mac 2011
- Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 1
- Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2
- Word Automation Services on Microsoft SharePoint Server 2013
- Microsoft Office Web Apps 2010 Service Pack 1
- Microsoft Office Web Apps 2010 Service Pack 2
- Microsoft Office Web Apps Server 2013

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

DESCRIPTION:

The vulnerability is a remote code execution vulnerability. The issue is caused when Microsoft Word parses specially crafted RTF-formatted data causing system memory to become corrupted in such a way that an attacker could execute arbitrary code. The vulnerability could

be exploited through Microsoft Outlook only when using Microsoft Word as the email viewer. Note that by default, Microsoft Word is the email reader in Microsoft Outlook 2007, Microsoft Outlook 2010, and Microsoft Outlook 2013.

- An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. 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.
- In a web-based attack scenario, an attacker could host a website that contains a webpage that contains a specially crafted RTF file that is used to attempt to exploit this vulnerability. In addition, compromised websites and websites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these websites. Instead, an attacker would have to convince users to visit the website, typically by getting them to click a link in an email message or Instant Messenger message that takes users to the attacker's website.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems as soon as they are made available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider applying the Microsoft Fix it solution described in the KB article 2953095
- Consider viewing emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

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

<http://blogs.technet.com/b/msrc/archive/2014/03/24/microsoft-releases-security-advisory-2953095.aspx>

Others:

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

<http://www.net-security.org/secworld.php?id=16567>