

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:

10/09/2012

SUBJECT:

Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (MS012-064)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office Word that 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.

SYSTEMS AFFECTED:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack

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:

Two vulnerabilities have been discovered in Microsoft Word. The first vulnerability is *Rich Text Format (RTF) listid Use-After-Free* vulnerability that is caused by the way Microsoft Word improperly handles memory when parsing RTF files. The second vulnerability is a *Paragraph Property Exceptions (PAPX) section corruption* issue that is caused when Microsoft Word improperly handles memory when parsing specially crafted word files.

These vulnerabilities can be exploited by opening a malicious RTF or Word document received as an email attachment, or by visiting a website that is hosting a malicious RTF or Word document. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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 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/bulletin/ms12-064>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0182>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2528>

SecurityFocus:

<http://www.securityfocus.com/bid/55781>

<http://www.securityfocus.com/bid/55780>