

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:

05/08/2012

SUBJECT:

Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (MS12-029)

OVERVIEW:

A vulnerability has 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 2008 for Mac
- Microsoft Office 2011 for Mac
- 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:

An RTF mismatch vulnerability has been discovered in Microsoft Office Word. This vulnerability exists in the way that Microsoft Office Word parses specially crafted Rich Text Format (RTF) data. This vulnerability can be exploited by opening a malicious Rich Text Format (RTF) document received as an email attachment, or by visiting a website that is hosting a malicious RTF 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/ms12-029>

Security Focus:

<http://www.securityfocus.com/bid/53344>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0183>