

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:

10/08/2013

SUBJECT:

Multiple Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS13-085)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Excel that could result in remote code execution. Exploitation may occur if a user opens a specially crafted Office file using an affected version of Microsoft Excel or other affected Microsoft Office software. Successful exploitation of these vulnerabilities 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 Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT
- Microsoft Office for Mac 2011
- Microsoft Excel Viewer

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 memory corruption vulnerabilities have been identified in Microsoft Excel that could allow remote code execution (CVE-2013-3889 and CVE-2013-3890). These vulnerabilities are caused due to the way that Microsoft Excel handles specially crafted Excel files.

Successful exploitation of these vulnerabilities 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider implementing the workaround found in MS13-085:
- Install and configure MOICE to be the registered handler for .xls, .xlt, and .xla files
- Use **Microsoft Office File Block policy to prevent the opening of Excel binary files**
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- 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/bulletin/ms13-085>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3889>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3890>