

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:

11/13/2012

SUBJECT:

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS012-076)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office Excel, a spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation 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 Office 2008 for Mac
- Microsoft Office 2011 for Mac
- Microsoft Excel 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:

Four vulnerabilities have been discovered in Microsoft Excel. Three vulnerabilities (*Excel SerAuxErrBar Heap Overflow Vulnerability*, *Excel Memory Corruption Vulnerability*, and *Excel SST Invalid Length Use After Free*) are caused by the way that Microsoft Excel handles memory when opening specially crafted Excel files. A fourth vulnerability (*Excel Stack Overflow Vulnerability*) is caused when Microsoft Excel encounters a modified data structure while parsing a specially crafted Excel file, corrupting system memory in such a way that an attacker could execute arbitrary code.

These vulnerabilities can be exploited by opening a malicious Excel file received as an email attachment, or by visiting a website that is hosting a malicious Excel 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/ms12-076>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1885>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1886>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1887>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2543>

SecurityFocus:

<http://www.securityfocus.com/bid/56425>

<http://www.securityfocus.com/bid/56431>

<http://www.securityfocus.com/bid/56426>

<http://www.securityfocus.com/bid/56430>