

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:

4/12/2011

SUBJECT:

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution(MS11-021)

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 XP
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2004 for Mac
- Microsoft Office 2008 for Mac
- Microsoft Office 2011 for Mac
- Open XML File Format Converter for Mac
- Microsoft Excel Viewer
- Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007

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:

Nine vulnerabilities have been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. These vulnerabilities can be triggered by opening a specially crafted Excel file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Excel file as an email attachment. In the web based scenario, a user would have to open the specially crafted Excel file that is hosted on a website. When the user opens the Excel file, the attacker's supplied code will execute.

Details of these vulnerabilities are as follows:

- One vulnerability exists due to Microsoft Excel not properly allocating buffer space while parsing record information in a specially crafted Excel file.
- Five vulnerabilities exist due to Microsoft Excel encountering a memory handling error during the validation of record information while parsing a specially crafted Excel file. System memory will then be corrupted in such a way that an attacker could execute arbitrary code.
- One vulnerability exists due to Microsoft Excel not properly initializing a variable that is used as the length of a 'memcpy' operation while parsing a specially crafted Excel file. This condition can be exploited to cause a buffer overflow that leads to code execution under the security context of the logged-on user.
- One vulnerability exists due to Microsoft Excel not properly managing the members of a data structure while parsing a specially crafted Excel file.
- One vulnerability exists due to Microsoft Excel not properly managing data structures while parsing a specially crafted Excel file.

Successful exploitation of these vulnerabilities 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.

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 visit untrusted websites or follow links provided by unknown or untrusted sources.
- Remind users not to open email attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>

<http://support.microsoft.com/kb/2502786>

<http://support.microsoft.com/kb/2466169>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0097>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0098>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0101>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0103>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0104>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0105>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0978>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0979>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0980>

SecurityFocus:

<http://www.securityfocus.com/bid/46227>

<http://www.securityfocus.com/bid/46226>

<http://www.securityfocus.com/bid/46225>

<http://www.securityfocus.com/bid/47256>

<http://www.securityfocus.com/bid/47244>

<http://www.securityfocus.com/bid/47245>

<http://www.securityfocus.com/bid/47235>

<http://www.securityfocus.com/bid/47243>

<http://www.securityfocus.com/bid/47201>