

*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:**

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS12-030)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Office, specifically in Microsoft 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:**

1. Microsoft Office 2003
2. Microsoft Office 2007
3. Microsoft Office 2010
4. Microsoft Office 2008 for Mac
5. Microsoft Office 2011 for Mac

**RISK:**

**Government:**

1. Large and medium government entities: **High**
2. Small government entities: **High**

**Businesses:**

1. Large and medium business entities: **High**
2. Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Six vulnerabilities have been identified in Microsoft Office that could allow remote code execution. These vulnerabilities are cause due to the way that Microsoft Excel handles specially crafted Excel files. The following vulnerabilities are covered by this advisory:

- Excel File Format Memory Corruption Vulnerability (CVE-2012-0141)
- Excel File Format Memory Corruption in OBJECTLINK Record Vulnerability (CVE-2012-0142)
- Excel Memory Corruption Using Various Modified Bytes Vulnerability (CVE-2012-0143)
- Excel SXLI Record Memory Corruption Vulnerability (CVE-2012-0184)
- Excel MergeCell Record Heap Overflow Vulnerability (CVE-2012-0185)
- Excel Series Record Parsing Type Mismatch Could Result in Remote Code Execution Vulnerability (CVE-2012-1847)

These vulnerabilities could be exploited if a user opens a specially crafted Excel document. 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.

**RECOMMENDATIONS:**

The following actions should be taken:

1. Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
2. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
3. Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
4. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
5. Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

**REFERENCES:**

**Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/MRecordS12-030>

**SecurityFocus:**

<http://www.securityfocus.com/bid/53342>

<http://www.securityfocus.com/bid/53373>

<http://www.securityfocus.com/bid/53374>

<http://www.securityfocus.com/bid/53375>

<http://www.securityfocus.com/bid/53376>

<http://www.securityfocus.com/bid/53379>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0141>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0142>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0143>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0184>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0185>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1847>