

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:

12/14/2011

SUBJECT: Vulnerability in Microsoft Excel Could Allow Remote Code Execution (MS11-096)

OVERVIEW:

A vulnerability have been discovered in Microsoft Office Excel, a spreadsheet application. This vulnerability could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or accessed 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 2004 for Mac

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:

A vulnerability has been identified in Microsoft Excel that could allow remote code execution. This vulnerability exists due to the way Microsoft Excel handles certain unspecified objects in memory. This vulnerability can be exploited through an e-mail based scenario or a web based scenario. In an e-mail based scenario, an attacker could craft a specially crafted Excel file and distribute the file to users through e-mail. The user would then have to download and execute the file for the exploit to be triggered. In the Web based scenario, the exploit is automatically triggered when a user visits a website with a specially crafted Excel file.

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.

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.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Consider installing Microsoft's Office File Validation tool for Microsoft Excel 2003 and Excel 2007 (<http://www.microsoft.com/technet/security/advisory/2501584.msp>) which would prompt the user for files that fail the Office File Validation and a user would have to click through the warning messages to open them before any of these vulnerabilities are exploited.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms11-096>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3403>

Security Focus:

<http://www.securityfocus.com/bid/50954>