

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:

5/10/2011

SUBJECT:

Microsoft PowerPoint Could Allow Remote Code Execution (MS11-036)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft PowerPoint, a program used for creating presentations. These vulnerabilities can be exploited by opening a specially crafted PowerPoint file received as an email attachment, or by visiting a web site that is hosting a specially crafted PowerPoint file. Successful exploitation could allow an attacker to gain 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 2004 for Mac
- Microsoft Office 2008 for Mac
- Open XML File Format Converter 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:

Two vulnerabilities exist due to Microsoft PowerPoint not properly handling memory while parsing specially crafted PowerPoint files. As a result, PowerPoint may cause memory corruptions that could allow an attacker to execute remote code. These vulnerabilities can be exploited via an email attachment or through the Web. In an email-based scenario, the user would have to open the specially crafted PowerPoint presentation as an email attachment. In a Web based scenario, a user would visit a website and then open the specially crafted PowerPoint presentation that is hosted on the page.

Successful exploitation could allow an attacker to gain 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.

Please note that there are currently no updates available for Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, and Open XML File Format File Converter for Mac. Microsoft is currently testing the updates for these advisories and will issue them when testing is complete.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider installing Microsoft's Office File Validation tool for Microsoft PowerPoint 2003 and PowerPoint 2007 (<http://www.microsoft.com/technet/security/advisory/2501584.mspx>) 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.
- 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 e-mail attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-036.mspx>

Security Focus:

<http://www.securityfocus.com/bid/47699>

<http://www.securityfocus.com/bid/47700>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0036>