

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:

6/8/2010

SUBJECT:

Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (MS10-036)

OVERVIEW:

A vulnerability has been identified in Microsoft Office, Microsoft's business application suite. This vulnerability could allow remote code execution if a user opens a specially crafted Office document. The document 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
2007 Microsoft Office System

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 Office that could allow an attacker to take complete control of an affected system. This vulnerability can be triggered by opening a specially crafted Excel, PowerPoint, Publisher, Visio, or Word document and can be exploited via email or through the web.

In the email based scenario, the user would have to open the specially crafted document as an email attachment. In the web based scenario, a user would have to open the specially crafted document that is hosted on a website. 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.
- Remind users not to download or open files from un-trusted websites.

- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS10-036.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1263>

Secunia:

<http://secunia.com/advisories/40082/>