

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:

4/14/2010

SUBJECT:

Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (MS10-023)

OVERVIEW:

A vulnerability has been discovered in Microsoft Publisher, which could allow an attacker to take complete control of an affected system. Microsoft Publisher, a component of Microsoft Office, is an application that allows users to create marketing materials and other types of publications. Exploitation may occur if a user opens a specially crafted Publisher file. This document may be received as an email attachment, or downloaded via the Web. Successful exploitation may 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 Publisher 2002
Microsoft Office Publisher 2003
Microsoft Office Publisher 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:

A vulnerability exists in the Microsoft Office Publisher application that could allow an attacker to execute arbitrary code on an affected system. This remote code execution vulnerability is due to a boundary error in the Textbox item that is included in a Publisher 97 file. This vulnerability can be triggered by opening a specially crafted Publisher file (.PUB) and can be exploited via email or through the Web. In the email base scenario, the user would have to open the specially crafted Publisher file as an email attachment. In the Web based scenario, a user would have to open a specially crafted Publisher file that is hosted on a malicious web site. Successful exploitation may 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 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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/Ms10-023.msp>

Security Focus:

<http://www.securityfocus.com/bid/39347>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0479>

Secunia:

<http://secunia.com/advisories/39375/>

Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-10-069>