

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:

12/14/2010

SUBJECT:

Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (MS10-105)

OVERVIEW:

Seven vulnerabilities have been discovered in Microsoft Office, which is Microsoft's business application suite. These vulnerabilities can be exploited by opening a specially crafted Microsoft Office document received as an email attachment, or by visiting a website that is hosting a malicious Microsoft Office document. 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. Failed exploitation could result in denial-of-service conditions.

SYSTEMS AFFECTED:

- Microsoft Office XP
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office Converter Pack
- Microsoft Works 9

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:

Seven remote code execution vulnerabilities have been discovered in Microsoft Office. Specifically, the vulnerabilities are caused by Microsoft Office improperly parsing certain image file formats and performing insufficient data validation when rendering images. Details of these vulnerabilities are as follows:

CGM Image Converter Buffer Overrun Vulnerability

A remote code execution vulnerability exists in the way Microsoft Office allocates memory when handling Computer Graphics Metafile (CGM) images contained in an Office document.

PICT Image Converter Integer Overflow Vulnerability

A remote code execution vulnerability exists in the way Microsoft Office allocates memory when handling Apple graphic file format (PICT) images contained in an Office document.

TIFF Image Converter Vulnerabilities (Heap Overflow, Buffer Overflow, Memory Corruption)

Three remote code execution vulnerabilities exist in the way that Microsoft Office parses specially crafted

Tagged Image File Format (TIFF) images contained in an Office document.

FlashPix Image Converter Vulnerabilities (Buffer Overflow, Heap Corruption)

Two remote code execution vulnerabilities exist in the way that Microsoft Office parses specially crafted FlashPix (FPX) images contained in an Office document.

Successful exploitation of these vulnerabilities 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. Failed exploitation could result in denial-of-service conditions.

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.
- 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 un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-105.msp>

Security Focus:

<http://www.securityfocus.com/bid/45270>

<http://www.securityfocus.com/bid/45273>

<http://www.securityfocus.com/bid/45274>

<http://www.securityfocus.com/bid/45275>

<http://www.securityfocus.com/bid/45278>

<http://www.securityfocus.com/bid/45283>

<http://www.securityfocus.com/bid/45285>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3945>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3946>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3947>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3949>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3950>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3951>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3952>