

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:

12/8/2009

SUBJECT:

Vulnerability in WordPad and Office Text Converter Could Allow Remote Code Execution (MS09-073)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows WordPad and the Office Text Converter for the Word 97 file format that could allow a remote attacker to take complete control of a vulnerable system. WordPad and the Office Text Converter are installed by default and allow some applications to open Word documents even if the software product, Microsoft Word, is not installed. This vulnerability can be exploited when a user opens a specially crafted Word 97 document using the affected versions of WordPad or Microsoft Office Word. 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:

Windows 2000
Windows XP
Windows 2003 Server
Microsoft Office XP
Microsoft Office 2003
Microsoft Works 8.5

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 Windows WordPad and the Office Text Converter. This vulnerability affects WordPad and the Office Text Converter and could be exploited when a user opens a specially crafted Word 97 document (.doc or .wri file extensions). If Microsoft Word is installed, the .doc file will open by default in Word. However if the attacker uses the .wri file extension, the file would automatically open in WordPad. In a web based scenario, the user will be prompted to open the file as long as the user has not previously unchecked the "Always ask before opening this type of file". This vulnerability cannot be automatically exploited through email, the user needs to open a specially crafted attachment.

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.
- Do not open untrusted documents using WordPad or Word.
- 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 email attachments, download or open files from un-trusted websites.
- Unless there is a business need to do otherwise, consider blocking .wri and/or .doc files at the network perimeter until these patches can be applied.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/ms09-073.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2506>

Secunia:

<http://secunia.com/advisories/37580/>

SecurityFocus:

<http://www.securityfocus.com/bid/37216>