

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:

10/13/2010

SUBJECT:

Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (MS10-083)

OVERVIEW:

A vulnerability has been identified in Windows Shell and WordPad which could allow the execution of remote code. Windows Shell provides users with access to objects necessary for running applications and managing the Windows Operating System. WordPad is a word processor application that is included in Microsoft Windows. This vulnerability may be exploited by opening a malicious WordPad document received as an email attachment, or by visiting a website that is hosting a malicious WordPad 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.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Server 2008
- Windows 7
- Word Pad

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 WordPad and Windows Shell that could allow an attacker to take complete control of an affected system. This vulnerability exists due to the way WordPad and Windows Shell validate Microsoft COM (Component Object Model) objects. An attacker could leverage the WordPad issue by enticing a user to open a specially crafted WordPad file. The Windows Shell vulnerability can be leveraged by getting a user to select or open a specially crafted shortcut file on a network share.

This vulnerability may be exploited by opening a malicious WordPad document received as an email attachment, or by visiting a website that is hosting a malicious WordPad 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.

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 sources.
- 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.

ORIGINAL REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>

VUPEN:

<http://www.vupen.com/english/advisories/2010/2630>

Secunia:

<http://secunia.com/advisories/41786>

Security Focus:

<http://www.securityfocus.com/bid/40574>