

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:

04/10/2012

SUBJECT:

Vulnerability in Windows Could Allow Remote Code Execution (MS12-024)

OVERVIEW:

A new vulnerability has been reported in the Microsoft Windows operating system. Exploitation may occur if a user opens a specially crafted, signed portable executable (PE) file. In order to exploit this vulnerability, an attacker could append malicious code to a digitally signed portable executable file without invalidating the signature and convince a user to run or install the program. 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 Windows XP

Microsoft Vista

Microsoft Windows 7

Microsoft Windows Server 2003

Microsoft Windows Server 2008

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 Windows Authenticode Signature Verification function, or WinVerifyTrust, which is used for portable execution (PE) files. Authenticode is a digital signature format used to determine the origin and integrity of software. The Windows operating system uses this function to insure that portable executables are safe by performing both signature verification and trust verification for a given object. However, the vulnerability allows an attacker to embed code in a portable executable without invalidating the digital signature. In order to exploit this vulnerability, an attacker would need to craft a PE file in the manner described and convince a user to run or install the program.

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.
- 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://technet.microsoft.com/en-us/security/bulletin/ms12-024>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0151>

Security Focus:

<http://www.securityfocus.com/bid/52868>