

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:

Multiple Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (MS10-073)

OVERVIEW:

Two vulnerabilities have been identified in the Microsoft Windows Kernel-Mode driver which could allow for privilege escalation. Utilizing these vulnerabilities, an attacker could escalate privileges and execute arbitrary code with kernel-level privileges resulting in full control of the affected machine. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

Microsoft has reported that this vulnerability is being actively exploited at this time as part of the Stuxnet worm.

SYSTEMS AFFECTED:

Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2

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:

Two vulnerabilities have been identified in the Microsoft Windows Kernel-Mode driver (win32.sys) which could allow for privilege escalation. The 'win32.sys' kernel-mode device driver provides various functions such as the window manager, collection of user input, and screen output. The first vulnerability is caused because the driver fails to properly index a table of function pointers when loading a keyboard layout. The second vulnerability is caused due to a validation error when handling Window Class data.

Utilizing these vulnerabilities, an attacker could escalate privileges and execute arbitrary code with kernel-level privileges resulting in full control of the affected machine. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

Microsoft has reported that this vulnerability is being actively exploited at this time as part of the Stuxnet worm.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

- 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.
- Ensure that anti-virus signatures are up-to-date.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms10-073.msp>

<http://support.microsoft.com/kb/981957>

Security Focus:

<http://www.securityfocus.com/bid/43773>

<http://www.securityfocus.com/bid/43774>

CNET:

http://news.cnet.com/8301-27080_3-20019353-245.html

Secunia:

<http://secunia.com/advisories/41471/>

<http://secunia.com/advisories/41775/>

H-Online:

<http://www.h-online.com/security/news/item/Microsoft-Patch-Tuesday-One-Stuxnet-hole-remains-open-1106886.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2743>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2744>