

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:

10/11/2011

SUBJECT:

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS11-077)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows Kernel-Mode Driver. Exploitation of any of these vulnerabilities could result in the escalation of privileges, create Denial of Service conditions, or execute arbitrary code with kernel-level privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system 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: Low

DESCRIPTION:

Four vulnerabilities have been identified in the Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for privilege escalation, remote code execution, or Denial of Service. The "win32.sys" kernel-mode device driver provides various functions such as the window manager, collection of user input, and screen output.

Win32k Null Pointer De-reference Vulnerability

An elevation of privilege vulnerability exists in the way that Windows kernel-mode drivers validate data supplied from user mode to kernel mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

Win32k TrueType Font Type Translation Vulnerability

A denial of service vulnerability exists in implementations of Microsoft Windows when the system improperly processes a specially crafted TrueType font file. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

Font Library File Buffer Overrun Vulnerability

The most severe of these vulnerabilities is due to improper handling of a specially crafted .fon font file. The vulnerability could allow an attacker to run code in kernel-mode and then install programs; view, change, or delete data; or create new accounts with full administrative rights. For a remote attack to be

successful, a user must visit a remote file system location or WebDAV share and open the specially crafted font file, or open the file as an e-mail attachment.

Win32k Use After Free Vulnerability

Microsoft Windows Kernel 'Win32k.sys' is prone to a local privilege-escalation vulnerability that occurs in the Windows kernel due to a use-after-free error. A local attacker can exploit this issue to execute arbitrary code with kernel-level privileges. Successful exploits will result in the complete compromise of affected computers. Failed exploit attempts may cause a denial-of-service condition.

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.
- Apply the principle of Least Privilege to all services.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-077.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1985>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2002>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2003>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2011>

SecurityFocus:

<http://www.securityfocus.com/bid/49973>

<http://www.securityfocus.com/bid/49975>

<http://www.securityfocus.com/bid/49981>