

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:

07/09/2013

SUBJECT:

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS13-053)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows Kernel-Mode drivers that could allow for remote code execution. The kernel mode drivers control window displays, screen output, and input from devices that the kernel passes to applications. Exploitation of these vulnerabilities could result in the execution of arbitrary code with full system 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:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows server 2012

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:

Seven vulnerabilities have been identified in Microsoft Windows Kernel-Mode driver (Win32k) that could allow for local privilege escalation through a non-administrative account running a specially crafted program. The list of vulnerabilities are as follows:

- Win32k Memory Allocation Vulnerability – (CVE-2013-1300)
- Win32k Dereference Vulnerability – (CVE-2013-1340)
- Win32k Vulnerability – (CVE-2013-1345)
- Win32k Information Disclosure Vulnerability – (CVE-2013-3167)
- Win32k Buffer Overflow Vulnerability – (CVE-2013-3172)
- Win32k Buffer Overwrite Vulnerability – (CVE-2013-3173)
- Win32k Read AV Vulnerability – (CVE-2013-3660)

An additional vulnerability has been identified due to the improper handling of TrueType Fonts (TTF) that could allow for remote privilege escalation.

These vulnerabilities may be exploited by multiple methods:

Web browsing attack scenario - an attacker could create a webpage that is used to exploit this vulnerability. For successful exploitation, a user must visit the webpage, or click on a link in an email.

Email attachment attack scenario - a specially crafted file that takes advantage of this vulnerability can be sent as an email attachment. In order for exploitation to be successful, the user must open the attachment.

Local user attack scenario – a malicious user logs onto the system and runs a specially crafted program to escalate his account privileges.

Successful exploitation of any of these vulnerabilities could result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full administrative rights.

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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-053>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1300>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1340>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1345>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3129>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3172>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3167>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3173>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3660>