

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:

10/08/2013

SUBJECT:

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS13-081)

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 Server 2008
- Windows Server 2012
- Windows RT
- Windows Vista
- Windows 7
- Windows 8

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 privately reported in Microsoft Windows that could allow for remote code execution. Successful exploitation of these vulnerabilities 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.

- **OpenType Font Parsing Vulnerability (CVE-2013-3128)** A remote code execution vulnerability exists in the way Windows handles specially crafted OpenType fonts (OTF). To exploit this vulnerability, a user would have to visit a malicious website containing a specially crafted OTF file.
- **TrueType Font CMAP Table Vulnerability (CVE-2013-3894)** A remote code execution vulnerability exists in the way that Windows handles specially crafted TrueType fonts (TTF). To exploit this vulnerability, a user would have to visit a malicious website containing a specially crafted TTF file.
- **Windows USB Descriptor Vulnerability (CVE-2013-3200)** An elevation of privilege vulnerability exists as a result of how object memory is handled by Windows USB drivers, potentially allowing for the execution of arbitrary code. In order to exploit this vulnerability a malicious USB device would need to be inserted into a vulnerable workstation.
- **Win32k Use After Free Vulnerability (CVE-2013-3879)** An elevation of privilege vulnerability exists as a result of how object memory is handle by Windows kernel-mode driver, potentially allowing for the execution of arbitrary code. Local access to a vulnerable workstation is required to exploit this issue.
- **App Container Elevation of Privilege Vulnerability (CVE-2013-3880)** An elevation of privilege vulnerability exists in the Windows App Container, possibly allowing for the disclosure of information on the local system from within the App Container.
- **Win32k NULL Page Vulnerability (CVE-2013-3881)** An elevation of privilege vulnerability exists as a result of how objects in memory are handled by the Windows kernel-mode driver, potentially allowing for the execution of arbitrary code. Local access to a vulnerable workstation is required to exploit this issue.
- **DirectX Graphics Kernel Subsystem Double Fetch Vulnerability (CVE-2013-3888)** An elevation of privilege vulnerability exists as a result of how objects in memory are handled by the Microsoft DirectX graphics kernel subsystem (dxgkrnl.sys), potentially allowing for the execution of arbitrary code. Local access to a vulnerable workstation is required to exploit this issue.

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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-081>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3128>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3894>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3200>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3879>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3880>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3881>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-3888>