

*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.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

02/10/2015

**SUBJECT:**

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS15-10)

**EXECUTIVE SUMMARY:**

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.

**THREAT INTELLIGENCE**

There are no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows RT
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

**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**

**TECHNICAL SUMMARY:**

Six vulnerabilities have been privately reported in Microsoft Windows that could allow for remote code execution.

- An elevation of privilege vulnerability exists in the Windows kernel-mode driver (Win32k.sys) that is caused when it improperly handles objects in memory. (CVE-2015-0003) (CVE-2015-0057)
- A security feature bypass vulnerability exists in the Cryptography Next Generation (CNG) kernel-mode driver (cng.sys) when it fails to properly validate and enforce impersonation levels. (CVE-2015-0010)
- An elevation of privilege vulnerability exists in the Windows kernel-mode driver (win32k.sys) due to a double-free condition. (CVE-2015-0058)
- A remote code execution vulnerability exists in the Windows kernel-mode driver (Win32k.sys) that is caused when it improperly handles TrueType fonts. (CVE-2015-0059)
- A denial of service vulnerability exists in the Windows kernel-mode driver (Win32k.sys) that is caused when the Windows font mapper attempts to scale a font. (CVE-2015-0060)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could 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.
- 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:**

<https://technet.microsoft.com/library/security/MS15-010>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0003>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0010>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0057>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0058>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0059>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0060>

#### **TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>