

*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:**

01/12/2016

**SUBJECT:**

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS16-005)

**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. Successful exploitation of these vulnerabilities could lead to an Address Space Layout Randomization (ASLR) bypass, and handling of objects in memory could allow for execution of remote code in the context of the logged on user. Depending on the privileges associated with the user, an attacker may install applications, view, change, or delete data or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

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

**SYSTEMS AFFECTED:**

- Windows Server 2008, 2008 R2 and Server Core installations
- Windows Server 2012, 2012 R2 and Server Core installations
- Windows RT, RT 8.1
- Windows Vista
- Windows 7
- Windows 8, 8.1
- Windows 10

**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:**

Two vulnerabilities were discovered in Microsoft Windows operating systems. The most severe of these vulnerabilities could allow for remote code execution. The vulnerabilities are as follows:

- Security feature bypass vulnerability exists in the way that the Windows graphics device interface handles objects in memory, allowing an attacker to retrieve information that could lead to an Address Space Layout Randomization (ASLR) bypass. (CVE-2016-0008)
- Remote code execution vulnerability exists in the way that Windows handles objects in memory. Successful exploitation of this vulnerability could run arbitrary code on a target system in the context of the logged on user. (CVE-2016-0009)

Successful exploitation of these vulnerabilities could lead to an Address Space Layout Randomization (ASLR) bypass, and handling of objects in memory could allow for execution of remote code in the context of the logged on user. Depending on the privileges associated with the user, an attacker may install applications, 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/MS16-005>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0008>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0009>

#### **TLP: WHITE**

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

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