

*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:**

11/10/2015

**SUBJECT:**

Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (MS15-115)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Windows that could allow for remote code execution. Exploitation of these vulnerabilities could result in the execution of remote 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 Vista
- Windows 7
- Windows Server 2008, R2, and Server Core Installation
- Windows Server 2012, R2, and Server Core Installation
- Windows RT, 8.1
- 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:**

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

- Two Kernel Memory Elevation of Privilege vulnerabilities have been found in the way Windows handles objects in memory. Successful exploitation would give the attacker the ability to run remote code with full user rights. (CVE-2015-6100, CVE-2015-6101)
- Two Kernel Memory Information Disclosure vulnerabilities exist due to a failure to properly initialize memory addresses. Successful exploitation would give the attacker access to the base address of the Kernel driver from a compromised process. (CVE-2015-6102, CVE-2015-6109)
- One Kernel Security Feature Bypass vulnerability exists due to a failure to properly initialize memory addresses. Successful exploitation would give the attacker access to the base address of the Kernel driver from a compromised process. (CVE-2015-6113)
- Two Graphics Memory Remote Code Execution vulnerabilities exist due to a failure to properly validate permissions, allowing an account to inappropriately interact with the filesystem from low integrity level user-mode applications. Successful exploitation would give the attacker the ability to modify files outside of a low integrity level application. (CVE-2015-6103, CVE-2015-6104)

Successful exploitation could allow an attacker to gain 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.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches or workaround 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/en-us/library/security/ms15-115.aspx>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6100>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6101>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6102>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6103>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6104>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6109>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-6113>

**TLP: WHITE**

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

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