

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:**

03/10/2015

**03/11/2015 – Updated**

**SUBJECT:**

Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (MS15-020)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Windows 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. This vulnerability can be exploited when a user opens a specially crafted website, file or opens a file in a working directory that contains a specially crafted DLL file. 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.

**March 11 – UPDATED THREAT INTELLIGENCE:**

***The vulnerability captured in CVE-2015-0096 is reported to be one that was widely used as part of Stuxnet, and was not correctly patched back in 2010 as part of CVE-2010-2568. ICS systems utilizing Windows should be patched as well, after appropriate testing.***

**SYSTEM AFFECTED:**

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server Core
- Windows RT
- Windows RT 8.1
- 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:**

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

- A remote code execution exists in Windows Text Services when it improperly handles objects in memory. This vulnerability may be exploited if an attacker convinces a user to open a specially crafted website or file. (CVE-2015-0081)
- A remote code execution exists in Microsoft Windows when DLL files are improperly handled. This vulnerability may be exploited if an attacker convinces a user to open a file in the same directory as a specially crafted DLL file. (CVE-2015-0096)

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.

**March 11 - UPDATED RECOMMENDATIONS:**

*The following actions should be taken:*

- *ICS systems utilizing Windows should be patched as well, after appropriate testing.*

**REFERENCES:**

Microsoft:

<https://technet.microsoft.com/library/security/MS15-020>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0081>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2015-0096>

**March 11 - UPDATED REFERENCES:**

HP:

<http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/CVE-2015-0096-issue-patched-today-involves-failed-Stuxnet-fix/ba-p/6718402#.VQA-XvzF8ut>

[http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/StuxNOT-Zero-Day-Protection-from-HP-TippingPoint/ba-p/6718453#.VQA9t\\_zF8us](http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/StuxNOT-Zero-Day-Protection-from-HP-TippingPoint/ba-p/6718453#.VQA9t_zF8us)

Brian Krebs:

<http://krebsonsecurity.com/2015/03/microsoft-fixes-stuxnet-bug-again/>

Threatpost:

<https://threatpost.com/patched-windows-machines-exposed-to-stuxnet-lnk-flaw-all-along>

**TLP: WHITE**

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

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

