

*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 Microsoft Windows Could Allow Remote Code Execution (MS16-007)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Windows that could allow for remote code execution. Exploitation of the most severe vulnerability 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.

**SYSTEMS AFFECTED:**

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

**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 reported in Microsoft Windows. The most severe vulnerabilities could allow for remote code execution. Details of these vulnerabilities are as follows:

- One Heap Corruption Remote Code Execution vulnerability exists due to how Microsoft DirectShow improperly validates user input. An attacker could exploit the vulnerability by sending a specially crafted link to the user and by convincing the user to open it. Successful

exploitation would give the attacker the ability to run remote code with full user rights. (CVE-2016-0015)

- Two DLL Loading Remote Code Execution vulnerabilities exist due to how Windows improperly validates input before loading dynamic link library (DLL) files. An attacker would first have to log on to the target system and then run a specially crafted application in order to exploit these vulnerabilities. Successful exploitation would give the attacker the ability to run remote code with full user rights. (CVE-2016-0016, CVE-2016-0018)
- Two DLL Loading Elevation of Privilege vulnerabilities exist due to how Windows improperly validates input before loading dynamic link library (DLL) files. An attacker would first have to log on to the target system and then run a specially crafted application in order to exploit these vulnerabilities. Successful exploitation could elevate their privileges on a targeted system. (CVE-2016-0014, CVE-2016-0020)
- One Security Bypass vulnerability exists due to a failure to prevent remote logon to accounts that have no passwords set on Windows 10 hosts running RDP services. An attacker could exploit this vulnerability by using an older version of the RDP client to connect to the Windows 10 host. The attacker could then log on as a user if the account has no password set despite the default system setting that restricts access to accounts without passwords to local logon only. Successful exploitation could allow an attacker to gain access to the remote host as another user, possibly with elevated privileges. (CVE-2016-0019)

Successful exploitation of the most severe vulnerabilities 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/ms16-007.aspx>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0014>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0015>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0016>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0018>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0019>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0020>

**TLP: WHITE**

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

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

