

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:

A Vulnerability in VBScript Scripting Engine Could Allow for Remote Code Execution (MS16-003)

OVERVIEW:

A vulnerability exists in the VBScript scripting engine in Microsoft Windows, which could allow for remote code execution. VBScript (Visual Basic Scripting Edition) is an active scripting language developed by Microsoft that is modeled on Visual Basic. Successful exploitation could result in an attacker gaining 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.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista Service Pack 2 - VBScript 5.7
- Windows Vista x64 Edition Service Pack 2 - VBScript 5.7
- Windows Server 2008 for 32-bit Systems Service Pack 2 - VBScript 5.7
- Windows Server 2008 for x64-based Systems Service Pack 2 - VBScript 5.7
- Windows Server 2008 for Itanium-based Systems Service Pack 2 - VBScript 5.7
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) - VBScript 5.7
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) - VBScript 5.7
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) - VBScript 5.8

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:

A vulnerability exists in the VBScript scripting engine in Microsoft Windows, which could allow for remote code execution if a user visits a specially crafted website or opens a maliciously crafted Office document. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or a Microsoft Office document that hosts the Internet Explorer rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit this vulnerability. (CVE-2016-0002)

The VBScript scripting engine is installed with supported releases of Microsoft Windows. In addition, installing a newer version of Internet Explorer on a system can change the version of the VBScript scripting engine that is installed. To determine which version of the VBScript scripting engine is installed on your system, perform the following steps:

1. Open Windows Explorer.
2. Navigate to the %systemroot%\system32 directory.
3. For VBScript, right-click vbscript.dll, select Properties, and then click the Details.
4. For JScript, right-click jscript.dll, select Properties, and then click the Details.
5. The version number is listed in the File Version field. If your file version starts with 5.8, for example 5.8.7600.16385, then VBScript 5.8 is installed on your system.

PLEASE NOTE: The affected software in this bulletin applies to systems without Internet Explorer installed, to systems with Internet Explorer 7 installed, and to Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) with Internet Explorer 8 installed. Customers with all other systems running Internet Explorer 8 or later should apply the Internet Explorer Cumulative Update (MS16-001), which also addresses the vulnerability discussed in this advisory.

Successful exploitation could result in an attacker gaining 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 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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

- A work around for CVE-2016-0002 is to restrict access to VBScript.dll. The command line instructions to accomplish this are available in Microsoft Security Bulletin MS16-003.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS16-003>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0002>

TLP: WHITE

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

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