



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 10, 2015

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2015-023

DATE(S) ISSUED:

03/10/2015

SUBJECT:

Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (MS15-019)

OVERVIEW:

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. 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. 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 is no known proof-of-concept code available at this time. Updates are available.

SYSTEM AFFECTED:

- Windows Server 2003 Service Pack 2 – VBScript 5.6 and 5.7
- Windows Server 2003 x64 Edition Service Pack 2 – VBScript 5.6 and 5.7
- Windows Server 2003 Service Pack 2 for Itanium-based Systems – VBScript 5.6 and 5.7
- Windows Vista Service Pack 2 – VBScript 5.7
- Windows Vista Service x64 Edition 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. 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. VBScript (Visual Basic Scripting Edition) is an Active Scripting language developed by Microsoft that is modeled on Visual Basic.

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:

- Open Windows Explorer.
- Navigate to the %systemroot%\system32 directory.
- Right-click vbscript.dll, select Properties, and then click the Details.

- o 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, and to systems with Internet Explorer 8 or earlier installed. Customers with systems running Internet Explorer 9 or later should apply the Internet Explorer Cumulative Update (MS15-018), 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:

We recommend the following actions be taken:

- Apply appropriate updates 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 download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS15-019>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0032>