

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.

DATE(S) ISSUED:

02/11/2014

SUBJECT:

Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (MS14-011)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in the VBScript scripting engine in Microsoft Windows. VBScript (Visual Basic Script) is an interpreted, object-based scripting language that is often used to make websites more flexible or interactive. This vulnerability can be exploited if a user visits a website with specially crafted content designed to take advantage of this vulnerability. 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. Failed exploit attempts may result in a denial-of-service condition.

THREAT INTELLIGENCE

At this time this vulnerability is not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- VBScript version 5.6 through 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 remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

To exploit this vulnerability an attacker hosts a specially crafted website and gets the user to visit the page. When the attacker's script is decoded, it can cause a memory corruption error in Internet Explorer, which will result in either a crash or the execution of remote code.

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. Failed exploit attempts may result in a denial-of-service condition.

By default, Internet Explorer on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 runs in a restricted mode that is known as Enhanced Security Configuration. This mitigates the risk of this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate patch 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 untrusted websites or follow links provided by unknown or untrusted sources.
- Configure Internet Explorer to prompt before running ActiveX Controls and Active Scripting in all zones.

REFERENCES:**Microsoft:**

<http://support.microsoft.com/kb/2928390>

<http://technet.microsoft.com/en-us/security/bulletin/MS14-011>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0271>