

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:

9/8/2009

SUBJECT:

Vulnerability in Microsoft JScript Scripting Engine Could Allow Remote Code Execution (MS09-045)

OVERVIEW:

A vulnerability exists in the way the Jscript scripting engine processes scripts within web pages. Jscript is a scripting language that is used to enhance the user experience when visiting web pages such as enabling animated content to be displayed. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit 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.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

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

DESCRIPTION:

A vulnerability exists in the way the JScript scripting engine decodes scripts which could allow a remote attacker to take complete control of an affected system. Scripting is used in web pages and server-side Active Server Pages (.ASP) to add features to web sites. JScript scripts can run only in the presence of an interpreter or host, such as Active Server Pages (ASP), Internet

Explorer, or Windows Script Host. Scripts embedded in web pages are often encoded to make it difficult for users to read. When the specially crafted script is decoded, and loaded into memory, a memory corruption error can occur causing Internet Explorer to either crash or execute 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.

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 un-trusted websites or follow links provided by unknown or un-trusted sources.
- Configure Internet Explorer to prompt before running ActiveX Controls and Active Scripting in all zones.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms09-045.msp>

<http://blogs.technet.com/srd/>

Security Focus:

<http://www.securityfocus.com/bid/36224>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1920>