

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:

03/12/2013

SUBJECT:

Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (MS13-022)

OVERVIEW:

A vulnerability has been discovered in the Microsoft Silverlight which could allow an attacker to take complete control of an affected system. Microsoft Silverlight is a web application framework that provides support for .NET applications and used for streaming media. The vulnerabilities can be exploited if a user visits or is redirected to a malicious web page, or runs a specially crafted Silverlight application.

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.

SYSTEMS AFFECTED:

Microsoft Silverlight 5

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 has been discovered in Microsoft Silverlight which could allow an attacker to take complete control of an affected system. The vulnerability is caused by Silverlight

incorrectly checking a memory pointer when rendering an HTML object. The vulnerability can be exploited by opening a specially crafted Silverlight web application.

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.

- Consider uninstalling Silverlight if there is no business need.

- Block Silverlight content at the organization's perimeter.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Apply the principle of Least Privilege to all services.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-022>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0074>

Security Focus:

<http://www.securityfocus.com/bid/58327>