

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:

07/09/2013

SUBJECT:

Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (MS13-052)

OVERVIEW:

Multiple vulnerabilities have been discovered in the Microsoft .NET Framework and Microsoft Silverlight which could allow an attacker to take complete control of an affected system. Microsoft .NET is a software framework for applications designed to run under Microsoft Windows. Microsoft Silverlight is a web application framework that provides support for .NET applications and used for streaming media.

These vulnerabilities can be exploited if a user visits or is redirected to a malicious web page, runs a specially crafted Microsoft .NET application 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:

- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows 7
- Windows 8
- Microsoft Silverlight 5 for Windows
- Microsoft Silverlight 5 for Mac
- Microsoft .NET Framework 4.5 and earlier for Windows

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:

Multiple vulnerabilities have been discovered in the Microsoft .NET Framework and Microsoft Silverlight which could allow an attacker to take complete control of an affected system.

Microsoft .NET Framework Vulnerabilities -

TrueType Font Parsing Vulnerability - CVE-2013-3129

A remote code execution vulnerability exists in the way that affected components handle specially crafted TrueType font files. The vulnerability could allow remote code execution if a user opens a specially crafted TrueType font file.

Array Access Violation Vulnerability - CVE-2013-3131

A remote code execution vulnerability exists in the way the .NET Framework handles multidimensional arrays of small structures.

Delegate Reflection Bypass Vulnerability - CVE-2013-3132

An elevation of privilege vulnerability exists in the way that .NET Framework validates the permissions of certain objects performing reflection. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Anonymous Method Injection Vulnerability - CVE-2013-3133

An elevation of privilege vulnerability exists in the way that the .NET Framework validates permissions for objects involved with reflection.

Array Allocation Vulnerability - CVE-2013-3134

A remote code execution vulnerability exists in the way that Microsoft .NET Framework allocates arrays of small structures.

Delegate Serialization Vulnerability - CVE-2013-3171

An elevation of privilege vulnerability exists in the way that the .NET Framework validates permissions for delegate objects during serialization.

Microsoft Silverlight Vulnerability –

Null Pointer Vulnerability - CVE-2013-3178

A remote code execution vulnerability exists in the way Microsoft Silverlight handles a dereference to a null pointer.

These vulnerabilities can be exploited if a user visits or is redirected to a malicious web page, runs a specially crafted Microsoft .NET application 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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- 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.
- Unless there is a business need to do otherwise, consider disabling Microsoft .NET applications.
- Unless there is a business need to do otherwise, consider disabling Microsoft Silverlight.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-052>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3129>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3131>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3132>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3133>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3134>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3171>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3178>