

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 10, 2010

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:

SA2010-052

DATE(S) ISSUED:

8/10/2010

SUBJECT:

Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (MS10-060)

OVERVIEW:

Two 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 SP3
- Windows Vista
- Windows Server 2003
- Windows Server 2008
- Windows 7
- Microsoft Silverlight
- Microsoft .NET Framework

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:

Two 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.

The first vulnerability is due to the way Microsoft Silverlight's ActiveX control handles pointers. The ActiveX control is identified by CLSID: DFEAF541-F3E1-4C24-ACAC-99C30715084A. An attacker can exploit this vulnerability by hosting a specially crafted webpage. Once the user visits or is redirected to the page, the vulnerability will allow the execution of arbitrary code in the application that uses the ActiveX control. Successful exploitation of these vulnerabilities could allow an attacker to gain 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.

The second vulnerability is a remote code execution vulnerability in Microsoft .NET Framework and Microsoft Silverlight. This vulnerability occurs within Microsoft .NET Common Language Runtime (CLR). This vulnerability can be exploited through several attack scenarios. In the first scenario, an attacker uploads malicious ASP.NET code to a web server that hosts user-created content. In this scenario, the attacker would gain the same privileges as the service account associated with the application pool identity. Depending on the privileges granted to the service account and on the application pool configuration, an attacker might be able to take control of other application pools on the affected system. In the second scenario, users can be exploited if they visit a specially crafted web site that hosts malicious XAML (Extensible Application Markup Language) content. In the third scenario, an attacker can exploit this issue by placing a malicious .NET application on a compromised network share. In the case of web-browsing or network share attack scenarios, successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the service account, 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 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 XAML browser applications in Internet Explorer.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-060.msp>

<http://www.microsoft.com/downloads/details.aspx?familyid=7e3f6c16-1339-49bc-a60c-ddc6c3a54850&displaylang=en>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0019>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1898>

Securityfocus:

<http://www.securityfocus.com/bid/42138>

<http://www.securityfocus.com/bid/42295>