



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

May 8, 2012

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:

SA2012-026

DATE(S) ISSUED:

5/08/2012

SUBJECT:

Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (MS12-034)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office, Microsoft Windows, the Microsoft .NET Framework, and Microsoft Silverlight. Microsoft Office is Microsoft's business application suite. 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.

The most severe of these vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a malicious webpage that embeds TrueType font files.

SYSTEMS AFFECTED:

- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows 7
- Microsoft .NET Framework 3.0
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Silverlight 4
- 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:**

Ten vulnerabilities have been discovered in Microsoft Office, Microsoft Windows, the Microsoft .NET Framework, and Microsoft Silverlight.

Two TrueType font parsing vulnerabilities exist due to the way that affected components handle specially crafted TrueType font files. These vulnerabilities can be exploited in three different ways. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. In a local attack scenario, an attacker could also exploit this vulnerability by running a specially crafted application to take complete control over the affected system.

A .NET framework buffer allocation vulnerability exists that can allow a Microsoft.NET Framework application to access memory in an unsafe manner. An attacker could exploit this vulnerability by hosting a website that contains a specially crafted XBAP (XAML browser application) that could exploit this vulnerability and then convince a user to view the website. This vulnerability could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions.

Two vulnerabilities exist in GDI+ that could allow remote code execution. Both vulnerabilities occur due to the way that GDI+ handles validation of EMF images. These vulnerabilities could be exploited if a user opens a special crafted EMF image or Office document.

A remote code execution vulnerability exists in Microsoft Silverlight that can allow a Silverlight application to access memory in an unsafe manner. This vulnerability may be exploited if a user visits a maliciously crafted web page.

Three elevation of privilege vulnerabilities exist in the way that the Windows kernel-mode driver manages the functions related to Windows and messages handling, keyboard layout files, and scrollbar calculation. To exploit these vulnerabilities, an attacker would first have to log on to the system. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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.

Lastly, a denial of service vulnerability exists due to the way that the .NET Framework compares the value of an index. This vulnerability could be exploited if an attacker sends

a small number of specially crafted requests to an affected site, causing a denial of service condition.

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.
- Do not click on URLs from unknown or untrusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-034>

Security Focus

<http://www.securityfocus.com/bid/53360>

<http://www.securityfocus.com/bid/53358>

<http://www.securityfocus.com/bid/53363>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0159>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0162>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0164>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0165>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0167>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0176>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0180>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0181>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1848>