



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

November 13, 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:
SA2012-074

DATE(S) ISSUED:
11/13/2012

SUBJECT:
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (MS12-074)

OVERVIEW:
Five vulnerabilities have been discovered in the Microsoft .NET Framework, some of 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. 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 loads a specially crafted proxy configuration file.

Successful exploitation of these vulnerabilities could allow the attacker to obtain complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft .NET Framework 1.0
- Microsoft .NET Framework 1.1
- Microsoft NET Framework 2.0
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5

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:**

Five vulnerabilities have been discovered in the Microsoft .NET Framework, details of which are described below:

Reflection Bypass Vulnerability (CVE-2012-1895) – A privilege escalation vulnerability exists in .NET Framework due to the improper validation of permissions for objects performing reflection. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code Access Security(CAS) restrictions.

Web Reflection Optimization Vulnerability (CVE-2012-4777) - An elevation of privilege vulnerability exists in the way that the .NET Framework validates permissions for objects involved with reflection. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code Access Security(CAS) restrictions.

Code Access Security Information Disclosure (CVE-2012-1896) – An information disclosure vulnerability exists in the Microsoft .NET Framework due to the improper sanitation of output when a function is called from partially trusted code. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code Access Security (CAS) restrictions. Successful exploitation could result in the disclosure of sensitive information.

.NET Framework Insecure Library Loading (CVE-2012-2519) – A remote code execution vulnerability exists in the way .NET restricts the path for loading external libraries. Exploitation may occur if an attacker convinces a user to open a .NET application that resides in the same directory as a specially crafted Dynamic Link Library (DLL) file.

Web Proxy Auto-Discovery Vulnerability (CVE-2012-4776) - A remote code execution vulnerability exists in the way that the .Net Framework retrieves the default web proxy settings. Exploitation may occur if an attacker performs a man in the middle attack and provides the end-user with a specially crafted proxy detection file that contains client-side code in the form of JavaScript.

Successful exploitation of these vulnerabilities could result in the execution of the attacker-supplied code and allow the attacker to obtain complete control of the affected system. 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.
- 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.
- Unless there is a business need to do otherwise, consider disabling XAML browser applications (XBAP) in Internet Explorer.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-074>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1895>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1896>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2519>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4776>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4777>

Security Focus:

<http://www.securityfocus.com/bid/56455>

<http://www.securityfocus.com/bid/56456>

<http://www.securityfocus.com/bid/56462>

<http://www.securityfocus.com/bid/56463>

<http://www.securityfocus.com/bid/56464>