



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

**October 14, 2014**

*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:**

SA2014-065

**DATE(S) ISSUED:**

10/14/2014

**SUBJECT:**

Vulnerabilities in .NET Framework Could Allow Remote Code Execution (MS14-057)

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in the Microsoft .NET Framework 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. 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 Vista
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012
- Windows 7
- Windows 8
- Windows RT
- Server Core Installation Option
- 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

**TECHNICAL SUMMARY:**

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

- .NET ClickOnce Elevation of Privilege Vulnerability (CVE-2014-4073) - An elevation of privilege vulnerability in .NET ClickOnce that could allow an attacker to compromise Internet Explorer and allow the ClickOnce installer process to run outside of Protected Mode with elevated privileges.
- .NET Framework Remote Code Execution Vulnerability (CVE-2014-4121) - A remote code execution vulnerability in .NET 4.0 and 4.5 that could allow a remote attacker to run code in the contexts of the .NET web application.
- .NET ASLR Bypass Vulnerability (CVE-2014-4122) - An ASLR bypass vulnerability in the .NET Framework that could allow an attacker to predict memory locations.

**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.

**REFERENCES:**

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms14-057.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4073>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4121>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4122>