



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

**September 8, 2015**

*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:  
SA2015-110**

**DATE(S) ISSUED:  
09/08/2015**

**SUBJECT:  
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (MS15-101)**

**OVERVIEW:**  
Multiple vulnerabilities have been discovered in the Microsoft .NET Framework, the most severe 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. Successful exploitation could allow an attacker to install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

**THREAT INTELLIGENCE:**  
The elevation of privilege vulnerability (CVE-2015-2504) has been publicly disclosed.

**SYSTEM AFFECTED:**

- Windows Vista
- Windows 7
- Windows 8 and Windows 8.1
- Windows Server 2008 (Server Core Installations are Affected)
- Windows Server 2012 (Server Core Installations are Affected)
- Windows RT

**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: Low**

#### **TECHNICAL SUMMARY:**

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

- **One Elevation of Privilege Vulnerability (CVE-2015-2504)** which could allow an attacker to take complete control of an affected system. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using a web browser capable of instantiating XBAPs. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code Access Security (CAS) restrictions. Successful exploitation of this vulnerability could allow the attacker to install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
- **One Denial of Service Vulnerability (CVE-2015-2526)** exists that is caused when .NET fails to properly handle certain specially crafted requests.

#### **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 XBAPs in Internet Explorer 6, 7, 8. By default, newer versions of Internet Explorer no longer allow XBAPs to run on Internet websites, but they still function in the Local Intranet and Trusted Zones.**

#### **REFERENCES:**

**Microsoft:**

<https://technet.microsoft.com/en-us/library/security/ms15-101>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2504>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2526>