



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

November 11, 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:

SA2014-076

DATE(S) ISSUED:

11/11/2014

SUBJECT:

Vulnerability in XML Core Services Could Allow Remote Code Execution (MS14-067)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in the Microsoft Core XML Services (MSXML), which could allow an attacker to take complete control of an affected system. Microsoft Core XML Services is software that allows users to develop XML based applications.

This vulnerability can be exploited if a user visits or is redirected to a malicious web page using Microsoft Internet Explorer. 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.

THREAT INTELLIGENCE

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Server 2003
- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 8
- Windows 8.1
- Windows RT

- Windows RT 8.1

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:**

A vulnerability has been discovered in Microsoft XML Core Services (MSXML). The vulnerability can be exploited by visiting a specially crafted website that is designed to invoke Microsoft XML Core Services (MSXML) through Internet Explorer.

Successful exploitation of this vulnerability could allow the attacker to could gain the same user rights as the current user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please Note: By default, all supported versions of Microsoft Outlook, Microsoft Outlook Express, and Windows Mail open HTML email messages in the Restricted sites zone. The Restricted sites zone, which disables script and ActiveX controls, helps reduce the risk of an attacker being able to use this vulnerability to execute malicious code. Internet Explorer on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability.

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 download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources

REFERENCES:**Adobe:**

<https://technet.microsoft.com/library/security/MS14-067>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4118>