



# State of Alaska State Security Office

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

January 8, 2013

*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:**

SA2013-001

**DATE(S) ISSUED:**

01/08/2013

**SUBJECT:**

Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (MS13-002)

**OVERVIEW:**

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. These vulnerabilities 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.

**SYSTEMS AFFECTED:**

- . Windows XP
- . Windows Server 2003
- . Windows Vista
- . Windows Server 2008
- . Windows 7
- . Windows 8
- . Windows RT
- . Windows Server 2012
- . Microsoft Office 2003
- . Microsoft Office 2007

**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:**

Two vulnerabilities exist in the way that Microsoft Windows parses XML content. These vulnerabilities may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user. This security update resolves two privately reported vulnerabilities in Microsoft XML Core Services. The vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. For successful exploitation to occur, a user will need to visit the website or click a link in an email message or Instant Messenger message that takes the user to the attacker's website.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after testing.
- Restrict access to msxml3.dll (per Microsoft Reference below)
- Restrict access to msxml6.dll (per Microsoft Reference below)
- Prevent the MSXML 5.0 ActiveX control from being run in Internet Explorer (per Microsoft Reference below)
- Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting to temporarily mitigate this vulnerability.
- 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.

**REFERENCES:**

**Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms13-002>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0006>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0007>