

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 10, 2010

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:

SA2010-051

DATE(S) ISSUED:

8/10/2010

SUBJECT:

Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS10-051)

OVERVIEW:

A vulnerability has been discovered in Microsoft XML Core Services which could allow remote code execution. Microsoft XML Core Services is installed by default on all Windows systems, and is used to enhance the user experience on web pages. This vulnerability may be exploited if a user visits, or is redirected to, a specifically crafted web page or opens a specially crafted HTML formatted email. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. If the user is logged in with administrative privileges, an attacker could then install programs; view, change, or delete; or create new accounts with user rights.

SYSTEMS AFFECTED:

- Windows XP SP3
- Windows Server 2003
- Windows Server 2008
- Windows Vista
- Windows 7

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:

A vulnerability has been discovered in Microsoft XML Core Services that could allow an attacker to take complete control of an affected system. The vulnerability exists in the way that Microsoft XML Core Services handles HTTP responses. This vulnerability could allow remote code execution if a user browses a Web site that contains specially crafted content or opens specially crafted HTML formatted e-mail. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. If the user is logged in with administrative privileges, an attacker could then install programs; view, change, or delete; or create new accounts with user rights.

It should be noted that, by default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode that is known as Enhanced Security Configuration. Enhanced Security Configuration is a group of preconfigured settings in Internet Explorer that can reduce the likelihood of a user or administrator downloading and running specially crafted Web content on a server. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to the Internet Explorer Trusted sites zone.

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.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS10-051.msp>

Security Focus:

<http://www.securityfocus.com/bid/42300>

Secunia:

<http://secunia.com/advisories/40893>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2561>