



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

October 14, 2009

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:

SA2009-059

DATE(S) ISSUED:

10/14/2009

SUBJECT:

Security Update of ActiveX Kill Bits (MS09-055)

OVERVIEW:

Microsoft has released a security update which addresses vulnerabilities discovered in multiple ActiveX controls. ActiveX controls are small programs or animations that are downloaded or embedded in Web pages which will typically enhance functionality and user experience. Many web design and development tools have built ActiveX support into their products, allowing developers to both create and make use of ActiveX controls in their programs. There are more than 1,000 existing ActiveX controls available for use today.

When vulnerabilities are discovered in ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user account, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

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:

Microsoft Internet Explorer includes a security feature which will prevent an ActiveX control from being loaded by using registry settings. This is commonly referred to as setting the 'kill bit' of an ActiveX component. Once the kill bit is set, the associated component can never be loaded.

These vulnerabilities could allow an attacker to take complete control of an affected system. These vulnerabilities may be exploited if a user visits a specifically crafted web page.

Successful exploitation of any of these vulnerabilities will result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user account, an attacker could then install programs; view, change, or delete data; or create new accounts.

This update will set the kill bits for the following Class Identifiers (CLSIDs):

ATL OWC - OWC9 RecordNavigationControl (msowc.dll)

CLSID - 0002E531-0000-0000-C000-000000000046

ATL OWC - OWC9 FieldList (msowc.dll)

CLSID - 4C85388F-1500-11D1-A0DF-00C04FC9E20F

ATL OWC - OWC9 ExpandControl (msowc.dll)

CLSID - 0002E532-0000-0000-C000-000000000046

ATL OWC - OWC10 RecordNavigationControl(owc10.dll)

CLSID - 0002E554-0000-0000-C000-000000000046

ATL OWC - OWC11 (owc11.dll)

CLSID - 0002E55C-0000-0000-C000-000000000046

Visio Viewer 2002-2007 (viewer.dll)

CLSID - 279D6C9A-652E-4833-BEFC-312CA8887857

Windows Live Mail Mail Object (msmail.dll)

CLSID - B1F78FEF-3DB7-4C56-AF2B-5DCCC7C42331

Windows Live Mail Mesg Table Object (msmail.dll)

CLSID - B1F78FEF-3DB7-4C56-AF2B-5DCCC7C42331

Windows Live Mail Mime Editor (mailcomm.dll)

CLSID - A9A7297E-969C-43F1-A1EF-51EBEA36F850

Windows Live Mail Message List (msmail.dll)

CLSID - DD8C2179-1B4A-4951-B432-5DE3D1507142

MSN Photo Upload Tool (MsnPUpld.dll)

CLSID – 4F1E5B1A-2A80-42ca-8532-2D05CB959537

Office Excel Add-in for SQL Analysis Services (ReportBuilderAddin.dll)

CLSID - 27A3D328-D206-4106-8D33-1AA39B13394B

CLSID - DB640C86-731C-484A-AAAF-750656C9187D

CLSID - 15721a53-8448-4731-8bfc-ed11e128e444}

CLSID - 3267123E-530D-4E73-9DA7-79F01D86A89F

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate security update provided by Microsoft to vulnerable systems immediately after appropriate testing: <http://support.microsoft.com/kb/973525>
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS09-055.msp>

<http://www.microsoft.com/technet/security/bulletin/ms09-035.msp>

<http://www.microsoft.com/technet/security/bulletin/ms09-032.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493>

Security Focus:

<http://www.securityfocus.com/bid/35828>