



**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:

SA2009-060

DATE(S) ISSUED:

10/14/2009

SUBJECT:

Vulnerabilities in Microsoft ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (MS09-060)

OVERVIEW:

Three vulnerabilities have been discovered in Microsoft Office ActiveX controls that could allow an attacker to take complete control of an affected system or disclose information. ActiveX controls are small programs or animations that are downloaded or embedded in Web pages or Windows applications which will typically enhance functionality and user experience. Exploitation may occur if a user visits a specifically crafted web page or opens a file which takes advantage of these vulnerabilities. Successful exploitation of two vulnerabilities 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. Successful exploitation of the remaining vulnerability could result in the attacker obtaining information that would normally be accessible by the logged in user.

Please note: Public exploit code is available and one or more of these vulnerabilities are being actively exploited.

SYSTEMS AFFECTED:

- Microsoft Outlook
- Microsoft Visio Viewer
- Microsoft DHTML Editing Component ActiveX Control
- Microsoft Microsoft MSWebDVD ActiveX Control
- Microsoft Outlook Express
- Microsoft Visual C++
- Microsoft Visual Studio
- Microsoft Windows Media Player
- Microsoft Windows Live Messenger
- Microsoft Windows 2000

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows XP

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:

Three vulnerabilities associated with Microsoft Office ActiveX controls due to Microsoft's implementation of Active Template Library (ATL) have been discovered. ATL allows a developer the ability to create custom objects to quickly interface with Component Object Model (COM) features, such as ActiveX controls. These vulnerabilities can be exploited when a user visits a specially crafted web page or opens a specially crafted file.

Please note: Public exploit code is available and one or more of these vulnerabilities are being actively exploited.

ATL Uninitialized Object Vulnerability

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to an issue in the ATL headers that could allow an attacker to force the 'VariantClear()' function to be called on a VARIANT that has not been correctly initialized. VARIANT is a datatype used to pass information between programs. The 'VariantClear()' function can be manipulated by an attacker when the function is called during the handling of errors by supplying a corrupt data stream. 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.

ATL COM Initialization Vulnerability

A remote code execution vulnerability exists in the Microsoft Active Template Library (ATL) due to issues in the ATL headers that handle instantiation of an object from data streams. This would allow for unsafe usage of the 'OleLoadFromStream()' method that could allow the instantiation of arbitrary objects which can bypass related security policies, such as kill bits within 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.

ATL Null String Vulnerability

An information disclosure vulnerability exists in the Microsoft Active Template Library (ATL) that could allow a string to be read without a terminating NULL character. An attacker can take advantage of the vulnerability to read extra data beyond the end of the string and disclose information in memory. From the information gathered, the attacker may launch more targeted attacks. This vulnerability does not allow the attacker to execute code or be granted read access beyond what the logged in user is entitled to.

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.
- Configure Internet Explorer to prompt before running ActiveX Controls or disable ActiveX controls in the Internet Zone.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS09-060.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0901>

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

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2495>

Secunia:

<http://secunia.com/advisories/35967>

<http://secunia.com/advisories/37005>

<http://secunia.com/advisories/36997>

Security Focus:

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

<http://www.securityfocus.com/bid/35830>

<http://www.securityfocus.com/bid/35832>