



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

July 13, 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:

SA2009-033

DATE(S) ISSUED:

7/13/2009

7/14/2009 - UPDATED

8/11/2009 - UPDATED

SUBJECT:

Vulnerability in Microsoft Office Web Components ActiveX Control Could Allow Remote Code Execution

ORIGINAL OVERVIEW:

A vulnerability has been discovered in the Microsoft Office Web Components Spreadsheet ActiveX control that could allow a remote attacker to take complete control of a vulnerable system. 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. When vulnerabilities are discovered in ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation may 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.

There are confirmed reports that this vulnerability is being used for specific targeted attacks. More widespread exploitation may occur when additional details regarding this vulnerability become available.

There is no patch available at this time.

August 11 UPDATED OVERVIEW

Microsoft has released a patch for this vulnerability.

SYSTEMS AFFECTED:

- Microsoft Office XP Service Pack 3

- Microsoft Office 2003 Service Pack 3
- Microsoft Office XP Web Components Service Pack 3
- Microsoft Office 2003 Web Components Service Pack 3
- Microsoft Office 2003 Web Components for the 2007 Microsoft Office system Service Pack 1
- Microsoft Internet Security and Acceleration Server 2004 Standard Edition Service Pack 3
- Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition Service Pack 3
- Microsoft Internet Security and Acceleration Server 2006
- Internet Security and Acceleration Server 2006 Supportability Update
- Microsoft Internet Security and Acceleration Server 2006 Service Pack 1
- Microsoft Office Small Business Accounting 2006

August 11 UPDATED SYSTEMS AFFECTED

- **Microsoft BizTalk Server 2002**
- **Microsoft Visual Studio .NET 2003 Service Pack 1**
- **Microsoft Office Small Business Accounting 2006**

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

ORIGINAL DESCRIPTION:

A vulnerability has been discovered in the Microsoft Office Web Components Spreadsheet ActiveX control (OWC10.dll and OWC11.dll). Microsoft Office Web Components are ActiveX controls that provide Microsoft Office functionality, such as spreadsheets, tables, and charts. This vulnerability may be exploited if a user visits a maliciously crafted web page. Successful exploitation may result in an attacker gaining user level privileges. 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. OCWC10.dll is installed by default with Microsoft Office XP, and both DLLs are installed by default with Microsoft Office 2003. OWC11 is also installed by default with Microsoft ISA Server and Microsoft Office Accounting and Business Contact Manager. OWC11 is an optional install with Microsoft Office 2007.

Microsoft has recommended preventing Office Web Components Library from running in Internet Explorer by issuing the kill bit for the following classids:

CLSID: 0002E541-0000-0000-C000-000000000046
CLSID: 0002E559-0000-0000-C000-000000000046

There are confirmed reports that this vulnerability is being used for specific targeted attacks. More widespread exploitation may occur when additional details regarding this vulnerability become available.

There is no patch available at this time.

July 14 UPDATED DESCRIPTION:

A list of domains that are exploiting this vulnerability has been published. It is recommended that these domains are blocked in order to prevent possible compromise. The published list of domains can be found at:
<http://isc.sans.org/diary.html?storyid=6739>

August 11 UPDATED DESCRIPTION

Microsoft has released a patch for this vulnerability.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.
- Set the kill bit on the Class Identifier CLSID - 0002E541-0000-0000-C000-000000000046; further instructions on how to set the kill bit can be found at the following location (<http://support.microsoft.com/kb/240797>).
- Set the kill bit on the Class Identifier CLSID - 0002E559-0000-0000-C000-000000000046; further instructions on how to set the kill bit can be found at the following location (<http://support.microsoft.com/kb/240797>).
- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Ensure that all anti-virus software is up to date with the latest signatures.

July 14 UPDATED RECOMMENDATIONS:

- To avoid possible compromise, we recommend blocking the domains identified as exploiting the vulnerability in the following SANS Diary:
<http://isc.sans.org/diary.html?storyid=6739>

August 11 UPDATED RECOMMENDATIONS:

- ***Apply the appropriate patch to vulnerable systems immediately after appropriate testing.***

ORIGINAL REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/973472.mspx>

<http://blogs.technet.com/srd/>

<http://blogs.technet.com/msrc/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1136>

July 14 UPDATED REFERENCES:

SANS:

<http://isc.sans.org/diary.html?storyid=6739>

August 11 UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms09-043.mspx>