

Sent: Wednesday, February 13, 2008 7:42 AM

To: AIO/CIO List; DTS IT Leaders Other

Cc: Takai, Teri@CIO

Subject: FW: MS-ISAC Advisory Vulnerability in Microsoft OLE Automation Could Allow Remote Code Execution Risk HIGH

The following message is being sent to IT Leaders and was sent earlier today to agency Information Security Officers, Operational Recovery Coordinators and their backups by the Information Security Office.

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER CYBER SECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2008-004

DATE ISSUED: 2/12/2008

SUBJECT: Vulnerability in Microsoft OLE Automation Could Allow Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in Microsoft Windows Operating system which could allow an attacker to take complete control of the affected system. The vulnerability can be exploited if a user visits a specifically crafted web page, views a malicious HTML email message, or opens a malicious Microsoft Office file. Successful exploitation will result in an attacker gaining the same user privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

SYSTEMS AFFECTED:

*Microsoft Windows 2000 Service Pack 4

*Microsoft XP Service Pack 2

*Microsoft XP Professional x64 Service Pack 1 and Service Pack 2 *Microsoft Server 2003 Service Pack 1 and Service Pack 2 *Microsoft Server 2003 x64 Service Pack 1

and Service Pack 2 *Microsoft Server 2003 x64 Service Pack 1 for Itanium-based Systems *Microsoft Server 2003 x64 Service Pack 2 for Itanium-based Systems

*Microsoft Windows Vista *Microsoft Windows Vista x64 *Microsoft Office 2004 for Mac

*Microsoft Visual Basic 6.0 Service Pack 6

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 new vulnerability has been identified in the Object Linking and Embedding (OLE)

Automation component of the Windows operating system. Object linking and embedding is a Windows protocol that allows an application to share data with or control another application. Examples of uses for OLE automation include drag and drop operations, embedding of multimedia content in Web pages and compound documents (documents consisting of information from different sources, generated 'on-the-fly'). Object Linking and Embedding is part of Microsoft's ActiveX technology. The Microsoft OLE Automation component fails to properly handle certain requests, which can cause memory corruption. The vulnerability can be exploited using several attack methods including users visiting a malicious web page using Internet Explorer, clicking on a link contained in an email or instant message. The vulnerability can also be exploited if a user opens a malicious Office document. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the system. If the user is logged in with administrator privileges, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

RECOMMENDATIONS:

We recommend the following actions be taken:

*Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing. <http://www.microsoft.com/technet/security/bulletin/ms08-008.msp>

*Logon to your systems as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. Employ the principle of least privilege when ever possible.

*Do not visit unknown or un-trusted Web sites or click on links provided in an email.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms08-008.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0065>

Secunia:

<http://secunia.com/advisories/28902/>

California Office of Information Security

(916) 445-5239

security@oispp.ca.gov

www.infosecurity.ca.gov/

This message is for the designated recipient only and may contain privileged or confidential information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the e-mail by you is prohibited.