



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

December 12, 2008

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.

DATE(S) ISSUED:

12/12/2008

12/17/2008 UPDATED WITH MORE INFO

SUBJECT:

Vulnerability in Microsoft Internet Explorer

ORIGINAL OVERVIEW:

A vulnerability has been discovered in Microsoft Internet Explorer 7 (IE 7) which could allow an attacker to take complete control of an affected system. Exploitation can occur if a user visits a webpage specifically crafted to take advantage of this vulnerability. Successful exploitation may result in an attacker gaining complete control of the affected system. 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. Failed exploit attempts may cause Internet Explorer 7 to crash.

It should be noted that this vulnerability is currently being exploited on the Internet and there is no patch available at this time.

December 12 UPDATED OVERVIEW:

Microsoft has indicated that Internet Explorer 5.01, Internet Explorer 6, and Internet Explorer 8 Beta on all supported versions of Windows are potentially affected by this vulnerability.

December 17 UPDATED OVERVIEW:

Microsoft has released out-of-band security bulletin MS08-078. This bulletin includes a newly released patch that mitigates the previously unpatched vulnerability in Internet Explorer.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 7.0
- Avaya CIE 1.0
- Avaya Messaging Application Server
- Microsoft Windows Vista
- Microsoft Windows Vista Business
- Microsoft Windows Vista Enterprise
- Microsoft Windows Vista Home Basic

- Microsoft Windows Vista Home Premium
- Microsoft Windows Vista Ultimate
- Microsoft Windows XP
- Microsoft Windows XP 64-bit Edition
- Microsoft Windows XP 64-bit Edition SP1
- Microsoft Windows XP 64-bit Edition Version 2003
- Microsoft Windows XP Embedded
- Microsoft Windows XP Embedded SP1
- Microsoft Windows XP Gold
- Microsoft Windows XP Home
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Home SP2
- Microsoft Windows XP Home SP3
- Microsoft Windows XP Media Center Edition
- Microsoft Windows XP Media Center Edition SP1
- Microsoft Windows XP Media Center Edition SP2
- Microsoft Windows XP Media Center Edition SP3
- Microsoft Windows XP Professional
- Microsoft Windows XP Professional SP1
- Microsoft Windows XP Professional SP2
- Microsoft Windows XP Professional SP3
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows XP Tablet PC Edition SP1
- Microsoft Windows XP Tablet PC Edition SP2
- Microsoft Windows XP Tablet PC Edition SP3

December 12 UPDATED Systems Potentially Affected:

- *Microsoft Internet Explorer 5.01 SP4*
- *Microsoft Internet Explorer 6.0*
- *Microsoft Internet Explorer 6.0 SP1*
- *Microsoft Internet Explorer 8.0 Beta 2*
- *Windows 2000 SP4*
- *Windows Vista Service Pack 1*
- *Windows Vista x64 Edition*
- *Windows Vista x64 Edition Service Pack 1*
- *Windows Server 2003 Service Pack 1*
- *Windows Server 2003 Service Pack 2*
- *Windows Server 2003 x64 Edition*
- *Windows Server 2003 x64 Edition Service Pack 2*
- *Windows Server 2003 with SP1 for Itanium-based Systems*
- *Windows Server 2003 with SP2 for Itanium-based Systems*
- *Windows Server 2008 for 32-bit Systems*
- *Windows Server 2008 for x64-based Systems*
- *Windows Server 2008 for Itanium-based Systems*

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:**

Internet Explorer 7 is susceptible to a remote code-execution vulnerability due to an unspecified buffer overflow which exists in the mshtml.dll library when processing XML tags. This occurs when the browser accepts two opening HTML '' elements in a row. If these faulty '' elements are used to reference an XML ID that binds XML data in the HTML code, then an HTML element with a 'src' attribute in the 'TransferFromSrc()' function can be used to corrupt memory. Exploitation can occur if a user visits a maliciously crafted webpage or html file. This vulnerability would allow the attacker to take control of the application and 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. Failed exploit attempts may result in a denial-of-service condition.

It should be noted that exploit code is publicly available and this vulnerability is currently being exploited on the Internet. We have tested the exploit code and verified that it does in fact cause a heap-based buffer overflow and allows arbitrary remote code execution. There is no patch available at this time.

December 12 UPDATED DESCRIPTION:

Microsoft has indicated that Internet Explorer 5.01, Internet Explorer 6, and Internet Explorer 8 Beta on all supported versions of Windows are potentially affected by this vulnerability.

December 17 UPDATED DESCRIPTION:

Microsoft has released out-of-band security bulletin MS08-078. This bulletin includes a newly released patch that mitigates the vulnerability in Internet Explorer and confirms that all versions of Internet Explorer are affected. Current reports indicate that this vulnerability is primarily being exploited through legitimate web servers which have been compromised via SQL Injection and are now hosting malicious content. Customers should apply the patch immediately after appropriate testing.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not download or open files from un-trusted websites.
- Consider blocking the following hosts at network perimeter unless there is a business need to do otherwise. Be advised that this is a temporary fix as the IP addresses and domain names may change: wwwyyyyy.cn

(121.12.104.88); sllwrnm5.cn (59.34.216.92); baikec.cn; oiuytr.net (222.76.212.179); laoyang4.cn; cc4y7.cn (121.10.107.233).

December 17 UPDATED RECOMMENDATION:

- **Apply the patch immediately after appropriate testing.**

REFERENCES:

McAfee Avert Labs:

<http://www.avertlabs.com/research/blog/index.php/2008/12/09/yet-another-unpatched-drive-by-exploit-found-on-the-web/>

PC World:

http://www.pcworld.com/article/155190/new_web_attack_exploits_unpatched_ie_flaw.html

CISCO:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=17236>

eEye Digital Security:

<http://research.eeye.com/html/alerts/zeroday/20081209.html>

SecurityFocus:

<http://www.securityfocus.com/bid/32721>

Robert McMillan:

<http://www.networkworld.com/news/2008/120908-new-web-attack-exploits-unpatched.html?fsrc=rss-security>

December 12 UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/961051.msp>

December 17 UPDATED REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS08-dec.msp>

<http://www.microsoft.com/technet/security/bulletin/ms08-078.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4844>