



Search for

[TechNet Home](#) > [TechNet Security](#) > [Security Advisories](#)

TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community

Microsoft Security Advisory (961051) Vulnerability in Internet Explorer Could Allow Remote Code Execution

Published: December 10, 2008 | Updated: December 15, 2008

Microsoft is continuing its investigation of public reports of attacks against a new vulnerability in Internet Explorer. Our investigation so far has shown that these attacks are only against Windows Internet Explorer 7 on supported editions of Windows XP Service Pack 2, Windows XP Service Pack 3, Windows Server 2003 Service Pack 1, Windows Server 2003 Service Pack 2, Windows Vista, Windows Vista Service Pack 1, and Windows Server 2008. Microsoft Internet Explorer 5.01 Service Pack 4, Microsoft Internet Explorer 6 Service Pack 1, Microsoft Internet Explorer 6, and Windows Internet Explorer 8 Beta 2 on all supported versions of Microsoft Windows are potentially vulnerable.

This update to the advisory contains information about a new workaround and a recommendation on the most effective workarounds.

The vulnerability exists as an invalid pointer reference in the data binding function of Internet Explorer. When data binding is enabled (which is the default state), it is possible under certain conditions for an object to be released without updating the array length, leaving the potential to access the deleted object's memory space. This can cause Internet Explorer to exit unexpectedly, in a state that is exploitable.

At this time, we are aware only of attacks that attempt to use this vulnerability against Windows Internet Explorer 7. Our investigation of these attacks so far has verified that they are not successful against customers who have applied the workarounds listed in this advisory. Additionally, there are mitigations that increase the difficulty of exploiting this vulnerability.

We are actively working with partners in our [Microsoft Active Protections Program](#) (MAPP) and our [Microsoft Security Response Alliance](#) (MSRA) programs to provide information that they can use to provide broader protections to customers. In addition, we're actively working with partners to monitor the threat landscape and take action against malicious sites that attempt to exploit this vulnerability. Current trending indicates that there may be attempts to utilize SQL Injection attacks against Web sites to load attack code on those Web sites. If you're a Web site operation, please review [Microsoft Security Advisory \(954462\)](#), which provides information on tools you can use to analyze your Web site's code to help protect against SQL Injection attacks.

We are actively investigating the vulnerability that these attacks attempt to exploit. We will continue to monitor the threat environment and update this advisory if this situation changes. On completion of this investigation, Microsoft will take the appropriate action to protect our customers, which may include providing a solution through a service pack, our monthly security update release process, or an out-of-cycle security update, depending on customer needs.

Microsoft continues to encourage customers to follow the "Protect Your Computer" guidance of enabling a firewall, applying all software updates and installing anti-virus and anti-spyware software. Additional information can be found at [Security at home](#).

Mitigating Factors:

- [Protected Mode](#) in Internet Explorer 7 and Internet Explorer 8 Beta 2 in Windows Vista limits the impact of the vulnerability.
- By default, Internet Explorer on Windows Server 2003 and Windows Server 2008 runs in a restricted mode that is known as [Enhanced Security Configuration](#). This mode sets the security level for the Internet zone to **High**. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted sites zone.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
- Currently known attacks cannot exploit this issue automatically through e-mail.

General Information

- [Overview](#)
- [Frequently Asked Questions](#)
- [Suggested Actions](#)

Resources:

- You can provide feedback by completing the form by visiting [Microsoft Help and Support: Contact Us](#).
- Customers in the United States and Canada can receive technical support from [Microsoft Product Support Services](#). For more information about available support options, see [Microsoft Help and Support](#).
- International customers can receive support from their local Microsoft subsidiaries. For more information about how to contact Microsoft for international support issues, visit [International Support](#).
- [Microsoft TechNet Security](#) provides additional information about security in Microsoft products.




Disclaimer:

The information provided in this advisory is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions:

- December 10, 2008: Advisory published
- December 11, 2008: Revised to include Microsoft Internet Explorer 5.01 Service Pack 4, Internet Explorer 6 Service Pack 1, Internet Explorer 6, and Windows Internet Explorer 8 Beta 2 as potentially vulnerable software. Also added more workarounds.
- December 12, 2008: Revised to correct operating systems that support Windows Internet Explorer 8 Beta 2. Also added more workarounds and a reference to Microsoft Security Advisory (954462).
- December 13, 2008: Revised to add the workaround, **Disable XML Island functionality**. Also, in a FAQ entry, clarified the list of recommended workarounds and added the blog post URL for recommended workarounds.
- December 15, 2008: Updated the workarounds, **Disable XML Island functionality** and **Disable Row Position functionality of OLEDB32.dll**.

[↑ Top of page](#)

 [Printer Friendly Version](#)  [Send This Content](#)  [Add To Favorites](#)

How would you rate the usefulness of this content ?

1 2 3 4 5

Poor Outstanding

Tell us why you rated the content this way. (optional)

[Manage Your Profile](#) | [Contact Us](#) | [Newsletter](#)

© 2008 Microsoft Corporation. All rights reserved. [Contact Us](#) | [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

