

[NT] Microsoft Internet Explorer Keyboard Shortcut Processing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00105.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:12:31 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Microsoft Internet Explorer Keyboard Shortcut Processing

SUMMARY

Due to a design error in the processing of keyboard shortcuts for certain security dialogs, attackers may trick users to execute arbitrary programs downloaded from the Internet.

DETAILS

Vulnerable Systems:

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- * Microsoft Windows XP Professional x64 Edition
- * Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- * Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with Service Pack 1 for Itanium-based Systems
- * Microsoft Windows Server 2003 x64 Edition family
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)
- * Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service

[NT] Microsoft Internet Explorer Keyboard Shortcut Processing

Pack 4

- * Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4 or on Microsoft Windows XP Service Pack 1
- * Internet Explorer 6 for Microsoft Windows XP Service Pack 2
- * Internet Explorer 6 for Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- * Internet Explorer 6 for Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- * Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition
- * Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition
- * Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Millennium Edition
- * Internet Explorer 6 Service Pack 1 on Microsoft Windows 98, on Microsoft Windows 98 SE, or on Microsoft Windows Millennium Edition

A vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to trick users into executing malicious files.

The vulnerability is caused due to a design error in the processing of keyboard shortcuts for certain security dialogs. This can e.g. be exploited to delay the file download dialog and trick users into executing a malicious ".bat" file after pressing the "r" key.

A successful attack may be outlined as:

1. Detect that the user is typing on the keyboard.
2. Redirect to a malicious ".bat" file.
3. In a new thread, force the browser to consume a large amount of CPU resources via a simple loop statement. This causes the upcoming file download dialog to be delayed.
4. The user eventually presses the "r" key which is a keyboard shortcut for opening the downloaded file. The download dialog has not yet been shown for the user when this event occurs.
5. The loop statement stops causing the download dialog to be visible and the keyboard shortcut event is processed.
6. The malicious ".bat" file is launched.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>>
CAN-2005-2829

Disclosure Timeline:

21/05/2005 – Vulnerability discovered
24/05/2005 – Vendor notified
20/06/2005 – Vendor confirms the vulnerability
13/12/2005 – Vendor issues patch
13/12/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vuln@xxxxxxxxxxx>> Secunia Research.

The original article can be found at:

<http://secunia.com/secunia_research/2005-7/advisory/>

http://secunia.com/secunia_research/2005-7/advisory/

The advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/6R00T0KEUQ.html>>

<http://www.securiteam.com/windowsntfocus/6R00T0KEUQ.html>

=====
This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[NT\] mIRC Local Buffer Overflow \(DDC Filter\)*](#)
 - Next by Date: [*\[NEWS\] BZFlag Server DoS*](#)
 - Previous by thread: [*\[NT\] mIRC Local Buffer Overflow \(DDC Filter\)*](#)
 - Next by thread: [*\[NEWS\] BZFlag Server DoS*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)