

[VulnWatch] Buffer Overflow in EF Commander 3.54

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-07/0053.html>

From: Peter Winter-Smith (peter4020_at_hotmail.com)

Date: 07/26/03

To: vulnwatch@vulnwatch.org, vuln@secunia.com, bugs@securitytracker.com

Date: Sat, 26 Jul 2003 00:32:00 +0000

Buffer Overflow in EF Commander 3.54

Url: <http://www.efsoftware.com>

"EF Commander is a file manager, archiver, viewer, FTP-client for the Windows 95/98/Me, Windows NT 4.0, Windows 2000 and Windows XP desktop. If you've ever used and liked Norton Commander, you'll like this dual-windowed program, which comes complete with bubble and online help. You can search directory trees and directories and perform actions, including Run, on files. You can also check file attributes and edit files with search-and-replace and drag-and-drop. Use the internal editor or associate one of your choosing to edit files, easily view files and configure the buttons to suit your needs, and get system and disk information with a click of the mouse."

- EFSoftware Website

Indeed it is quite remarkable, sporting a huge number of extra features which make the \$25.00 registration fee (when using paypal) a definite bargain!

See: <http://www.efsoftware.com/order/e.htm> for order information.

I have noticed that EF Commander 3.54 (and possibly earlier versions) are vulnerable to a buffer overflow in the FTP banner and other areas. These can be replicated as follows:

FTP Banner:

=====

(EF Commander 3.54 connected...)

PADDING EBP EIP

220 [508xA][4xB][4xX] // Totalling 516+4 Bytes

(Access violation when executing 0x58585858) // 4xX

When sending the overly long packet as the FTP banner, the overflow does not often take an immediate effect, however when sending it as

VulnWatch: [VulnWatch] Buffer Overflow in EF Commander 3.54

part of another response, it is immediate.

Potentially an attacker would be able to execute arbitrary code on the system of an unsuspecting user.

Since I would not have access to a computer for a while, I thought it best to contact the vendor, and release the advisory together, as I very much doubt that any trouble will come from the knowledge of this security hole, especially before a patch can be made known.

Please visit EFSsoftware's website:

<http://www.efsoftware.com>

And check for an updated version, greater than 3.54, which will doubtless be patched against this bug.

=====

Operating system and servicepack level:
Windows 9x/Me/NT Based

Software:
EF Commander 3.54 (Possibly Earlier Versions)

Under what circumstances the vulnerability was discovered:
Under a vulnerability search.

If the vendor has been notified:
Yes, concurrent with the release of this advisory.

How to contact you for further information:
I can always be reached at peter4020@hotmail.com

Please credit this find to:
Peter Winter-Smith

Thank you for your time,
-Peter

Hotmail messages direct to your mobile phone <http://www.msn.co.uk/msnmobile>