

[UNIX] Off-by-One Error in realpath (FreeBSD)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0013.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/05/03

To: list@securiteam.com

Date: 5 Aug 2003 14:05:42 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

Off-by-One Error in realpath (FreeBSD)

SUMMARY

An off-by-one error exists in the C library function `realpath(3)`. This is the same bug that was recently found in the <http://www.securiteam.com/unixfocus/5ZP010AAUI.html>> `wu-ftpd` ftpd server by Janusz Niewiadomski and Janusz Niewiadomski.

DETAILS

The OpenBSD ftp daemon does not use `realpath(3)` in a way that could be exploited, however a number of other system binaries also use the function. It is not currently known whether this bug results in an exploitable security hole on OpenBSD. Since the bug led to an exploitable hole in `wu-ftpd`, it is entirely possible that some program using `realpath(3)` under OpenBSD may be vulnerable to attack. For OpenBSD 3.3 and higher, the ProPolice stack protector should provide some protection from this bug, but this cannot be guaranteed.

This bug has been fixed in OpenBSD-current as well as the 3.2 and 3.3

Securiteam: [UNIX] Off-by-One Error in realpath (FreeBSD)

stable branches. Patches are available for OpenBSD 3.2 and 3.3.

Patch for OpenBSD 3.2:

<ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/3.2/common/015_realpath.patch>
ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/3.2/common/015_realpath.patch

Patch for OpenBSD 3.3:

<ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/3.3/common/001_realpath.patch>
ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/3.3/common/001_realpath.patch

For versions of OpenBSD prior to 3.2, users may simply fetch the current revision of realpath.c from:

<<ftp://ftp.OpenBSD.org/pub/OpenBSD/src/lib/libc/stdlib/realpath.c>>
<ftp://ftp.OpenBSD.org/pub/OpenBSD/src/lib/libc/stdlib/realpath.c> then rebuild and install libc with the new realpath.c.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Todd.Miller@courtesan.com>>
Todd C. Miller.

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.