

[UNIX] QuiXplorer Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0052.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/16/04

To: list@securiteam.com

Date: 16 Aug 2004 10:16:05 +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>

QuiXplorer Directory Traversal

SUMMARY

<<http://quixplorer.sourceforge.net/>> QuiXplorer is "a simple, but fully functional, file manager for websites. QuiXplorer allows you to browse the files and directories on your web server (with PHP4) (without using an external FTP-client)".

A vulnerability in the QuiXplorer allows remote attackers to retrieve arbitrary files that reside outside the bound HTML root directory.

DETAILS

Vulnerable Systems:

- * QuiXplorer version 2.3

Immune Systems:

- * QuiXplorer version 2.3.1

QuiXplorer does not apply filters on user inputs when a download is requested. The directory parameter is well filtered to check that it does not create a request that goes outside the authorized directories, but the item can contains parent directory references.

Securiteam: [UNIX] QuiXplorer Directory Traversal

Exploit:

By requesting a URL such as:

http://vuln/quixplorer_2_3/index.php?action=download&dir=&item=../../../../etc/passwd&order=name&srt=yes

Solution:

Upgrade to version 2.3.1 or newer.

ADDITIONAL INFORMATION

The information has been provided by <mailto:cb-publicbox@ifrance.com>

Cyrille Barthelemy.

=====

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.