

[NT] WinRAR Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0157.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/31/05

To: list@securiteam.com

Date: 31 May 2005 17:10:47 +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>

WinRAR Directory Traversal

SUMMARY

By supplying a special archive file name it is possible to cause WinRAR to extract files on a different directory then the directory the user has requested the files to be extracted to.

DETAILS

Vulnerable Systems:

- * WinRAR version 3.42 and prior

WinRAR adds some options to unpack files directly using left-click. The extracing files directly in the directory option allows you to store the files in a directory that takes the same name of the compressed file but without the extension. In the case were the filename is '...zip' and you use choose to use this option, the uncompressed data will be stored in the "../" directory.

Disclosure Timeline:

02/01/2005 – Bug discovered

16/01/2005 – Mail sent to the vendor

16/01/2005 – Vendor response

02/02/2005 – Advisory released

ADDITIONAL INFORMATION

The information has been provided by <mailto:ripe@7a69ezine.org> Albert Puigsech Galicia .

=====

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.