

[NT] WinRAR Buffer Overflow Vulnerability (Long Extension)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0065.html>

From: support@securiteam.com

Date: 01/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Jan 2003 15:10:01 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

WinRAR Buffer Overflow Vulnerability (Long Extension)

SUMMARY

<<http://www.rarlab.com/>> WinRAR is archive manager on Windows (GUI). When WinRAR opens, an archive that includes the "long file extension" in inside, buffer overflow occurs on the stack. This is a general exploitable Buffer Overflow. If WinRAR user opens a malicious archive file, it has the dangerous possibility, such as system destruction, virus infection, etc. This vulnerability exists only in "winrar.exe", it is not command line tool.

DETAILS

Vulnerable systems:

- * WinRAR version 3.10 and prior

Immune systems:

- * WinRAR version 3.11

When WinRAR opens an archive file, it displays the file list of archives on a ListView Control Window.

Securiteam: [NT] WinRAR Buffer Overflow Vulnerability (Long Extension)

If "long file extension" over 256 bytes exists in this file list, buffer overflow occurs (May be not only inside of archives but also in general files).

Then, RET address is in the offset of 260 from "." (Offset value includes the first ".").

Further, the ESP register points to the address of the offset 264 from ".", next area of the RET address.

If RET address is overwritten at the address of the "jmp ESP" and the next area was overwritten at an arbitrary binary code, the binary code can be executed.

Note:

File extension is data that is start from 0x2e and exclude 0x2e, 0x2f, 0x5c, 0x00.

Case of offset 260, may be not enough size of using for binary code at 3.00en and 2.90.

However, offset that can control EIP exists yet, without 260. However, those offset values are different per a version and language edition.

Version 3.00en, 2.90en and 2.90ja are 552, 3.00ja is 557, 3.10en is 692, and 3.10ja is 697.

Vendor status:

<<mailto:roshal@rarlab.com>> Eugene Roshal released at 17 January 2003 new version 3.11 of WinRAR which fixed this problem. Very fast response and fix.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nesumin@softhome.net>> nesumin.

=====

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.