

[NEWS] RAR Fails to Determine Actual File Size (DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0029.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/03

To: list@securiteam.com

Date: 14 Sep 2003 15:03:35 +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>

RAR Fails to Determine Actual File Size (DoS)

SUMMARY

<<http://www.rarsoft.com/>> WinRAR is "one of the most popular file compression utilities for Windows". WinRAR incorrectly determines the actual size of compressed files saved in .rar format by reading its header information. This could allow attackers to confuse programs using this value into thinking they are extracting a much smaller file than that which will be extracted.

DETAILS

Vulnerable systems:

- * WinRAR version 3.20 and prior
- * Unrar version 2.71 and prior

Recently 01 security managed to devise a technique to spoof the header and create a valid CRC checksum for it. From this, 01 security discovered that WinRAR only depended on its header information and CRC check sum to determine the size and integrity of .rar files.

Before uncompressing .rar files, WinRAR pre-allocates space according to

Securiteam: [NEWS] RAR Fails to Determine Actual File Size (DoS)

the actual file size specified in the header to avoid fragmentation. However, pre-allocation occurs without checking the available hard disk space.

Once allocation has been completed, it will go on extracting, even if the hard disk size is less than the size of the files.

01 security then discovered that even if WinRAR detected the header corruption WinRAR did not avoid the extraction process. This leads WinRAR to believe that the actual size is correct.

When it starts extracting it doesn't find any valid data in the archive and on the basis of it's header it attempts to extract 1 gigabyte of data and simply goes on writing "0x00" filling up valuable hard disk space.

Proof of concept:

The proof of concept is a valid .rar file that is just 100 bytes but its header has been forged to fool WinRAR into thinking that it is a 1-gigabyte file by forging its header and creating a valid CRC checksum.

The proof of concept of .rar file can be obtained from the following URL:
<<http://www.geocities.com/visitbipin/test123.zip>>
<http://www.geocities.com/visitbipin/test123.zip>.

Side note (UNIX):

01 security also tested it on a Linux machine with unrar 2.71, which comes with most distributions. Same unrar binary is used by anti-virus scanner.

Result is the following:

```
$ unrar x -v test123.rar
UNRAR 2.71 freeware Copyright (c) 1993-2000 Eugene Roshal
Extracting from test123.rar
Extracting MAIL.DWN
```

```
MAIL.DWN - CRC failed
```

```
Total errors: 1
```

As CRC failed, unrar will delete this file immediately but during the extraction, it will create nice 1GB file.

As 01 security wrote above, same unrar binary is used by anti-virus scanner (amavisd-new in this case), so this is creates a very nasty possibility of DoS attack on servers.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:door_hunt3r@blackcodemail.com> hUNTER 007.

=====

Securiteam: [NEWS] RAR Fails to Determine Actual File Size (DoS)

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.