

Full-Disclosure: RE: [Full-Disclosure] Winrar doesn't determine the actual size of compressed files

## RE: [Full-Disclosure] Winrar doesn't determine the actual size of compressed files

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-09/0348.html>

---

**From:** Rainer Gerhards ([rgerhards\\_at\\_hq.adiscon.com](mailto:rgerhards_at_hq.adiscon.com))

**Date:** 09/09/03

To: <[door\\_hUNT3R@blackcodemail.com](mailto:door_hUNT3R@blackcodemail.com)>, <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Date: Tue, 9 Sep 2003 14:45:46 +0200

This could have very bad implications on anti-virus software that extracts rar files. As a DoS, you could send, well, some copies of the 100 byte file... I'll try to see if that works with some of the stuff that we have. If it is not just WinRar, this could be *\*really\** bad...

Rainer

> -----Original Message-----

> *From:* Bipin Gautam [[mailto:door\\_hUNT3R@blackcodemail.com](mailto:door_hUNT3R@blackcodemail.com)]

> *Sent:* Tuesday, September 09, 2003 1:02 PM

> *To:* [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)

> *Subject:* [Full-Disclosure] Winrar doesn't determine the  
> actual size of compressed files

>

>

> ---[ about WinRAR]---

> Winrar (<http://www.rarsoft.com/>) is one of the most popular  
> file compression utilities for Windows.

>

> --[summary]---

> Winrar incorrectly determines the actual size of compressed  
> files saved in .rar format by reading it's header information.

>

> --[details]--

> Recently we managed to devise a technique to spoof the header  
> and creating a valid CRC checksum. Later we found that Winrar  
> only depends on it's 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 the actual file size specified in the header to  
> avoid fragmentation. But pre-allocation occurs without  
> checking the available hdd space. Then it goes extracting,  
> even if the hdd size is less than the size of the files. We  
> did a test by extracting 1GB files in a hdd with 700MB free space.

>

> Surprisingly, we later discover that even in detecting of

RE: [Full-Disclosure] Winrar doesn't determine the actual size of compressed files

Full-Disclosure: RE: [Full-Disclosure] Winrar doesn't determine the actual size of compressed files

- > *header corruption WinRAR doesn't enforce to avoid extraction*
- > *process. this lead WinRAR to believe that the actual size is*
- > *correct .We managed to exploit this and create a proof of*
- > *concept to demonstrate this problem by changing the actual*
- > *file size in it's header. 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 hdd space.*
- >
- > *--[Proof of concept]--*
- > *The proof of concept is a valid .rar file which is just 100*
- > *bytes but it's header has been forged to fool Winrar into*
- > *thinking that it's a 1 gigabyte file by forging it's header*
- > *and creating a valid CRC checksum. All versions of Winrar*
- > *(upto 3.20 – latest version till date) seem to be vulnerable.*
- >
- > *The proof of concept of .rar file can be obtained from the*
- > *following URL: <http://www.geocities.com/visitbipin/test123.zip>*
- > *If you extract the file Winrar will try to extract this 100*
- > *bytes .rar file trusting the information in it's header but*
- > *not on the basis of it's data integrity.*
- >
- > *--[Background Information]--*
- > *This bug was originally discovered by hUNT3R, a member of 01*
- > *Security Sumbission. The vendor was notified via email.*
- > *Further discussion took place in 01 Security Sumbission's*
- > *forum with the developer of Winrar (Eugene Roshal) :*
- > *URL: [http://www.ysgnet.com/phorum/read.php?f=1&i=341&t=324#reply\\_341](http://www.ysgnet.com/phorum/read.php?f=1&i=341&t=324#reply_341)*
- >
- > *---[about 01 security submission]---*
- > *01s.s is a small group having experience as security*
- > *specialists, programmers and system administrators*
- > *<http://www.ysgnet.com/hn>.*
- >
- >
- >
- >
- > *|.oÃ>\_Oo.hÃ»UNTER.oO\_Ã>o. |*
- > *Â§ !Â¹007Ã•Â°Ã¿Ã'Ã-Ã Ã ÃŸÃ°Ã•Ã'9\*Ã½Ã! ! â€¦j*
- >
- >
- >
- >
- > *Secure mail ---> <http://www.blackcode.com>*
- >
- >
- >
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>