

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/2003-09/0347.html>

From: Rainer Gerhards (rgerhards_at_hq.adiscon.com)

Date: 09/09/03

To: <door_hUNT3R@blackcodemail.com>, <full-disclosure@lists.netsys.com>

Date: Tue, 9 Sep 2003 14:49:31 +0200

tested with 3.20 – can't reproduce. It says "file is corrupt", I press "close" – nothing happened....

Rainer

> -----Original Message-----
> From: Bipin Gautam [mailto:door_hUNT3R@blackcodemail.com]
> Sent: Tuesday, September 09, 2003 1:02 PM
> To: 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 t