

Forum:[Hack Forums](#)

Thread: [WinRAR CVE-2018-20250 Exploit | Spread FAST](#)

Goldmouth - February 23, 2019, 8:24 pm

CVE-2018-20250

exploit for Extracting Code Execution From Winrar

poc by Ridter

how to use ?

you just need to install python 3.7, and prepare a evil file you want to run, set the values you want, this exp script will generate the evil archive file automatically!

<https://github.com/WyAtu/CVE-2018-20250>

Enjoy. ? ?

#Skyline - February 23, 2019, 8:26 pm

Now this is useful. Thank you for the share.

*****W0lf***** - February 23, 2019, 11:01 pm

yeap , thanks for the share it bro ...a good one! Happy spreading!

BTC - February 23, 2019, 11:20 pm

Happy spreading everybody! Thanks for the share.

I find it is still quite easy to tell when you've opened an infected winrar archive :P

naxster - February 24, 2019, 12:48 am

(Feb 24, 2019 12:20 AM)Apex Wrote: [\[CITE\]](#) Happy spreading everybody! Thanks for the share.

I find it is still quite easy to tell when you've opened an infected winrar archive :P

How can you tell? :)

I haven't tried this yet, but does something pop up and reveal that the created WinRAR is infected?

BTC - February 24, 2019, 1:21 am

(Feb 24, 2019 01:48 AM)naxster Wrote: [\[CITE\]](#) How can you tell? :)

I haven't tried this yet, but does something pop up and reveal that the created WinRAR is infected?

Read the readme in the github the OP linked.

It shows screenshots of the exploit in different stages.

R4NS0M - February 24, 2019, 1:33 am

(Feb 23, 2019 09:24 PM)?HOSTAH? Wrote: [\[CITE\]](#) CVE-2018-20250

exploit for Extracting Code Execution From Winrar

poc by Ridter

how to use ?

you just need to install python 3.7, and prepare a evil file you want to run, set the values you want, this exp script will generate the evil archive file automatically!

<https://github.com/WyAtu/CVE-2018-20250>

Enjoy. ? ?Thanks a lot!

naxster - February 24, 2019, 1:46 am

(Feb 24, 2019 02:21 AM)Apex Wrote: [\[CITE\]](#) Read the readme in the github the OP linked.

It shows screenshots of the exploit in different stages.
Just read it, yeah that's a big tell (not OPs fault though)...

But I'm a bit sceptic about step 4...

It says this and I quote "when he restart the computer, the hi.exe will run."

Soooo what happens if the person deletes the files before restarting the computer? And also won't the stub run if he run the .exe file? :/

BTC - February 24, 2019, 1:48 am

(Feb 24, 2019 02:46 AM)naxster Wrote: [\[CITE\]](#) Just read it, yeah that's a big tell (not OPs fault though)...

But I'm a bit sceptic about step 4...

It says this and I quote "when he restart the computer, the hi.exe will run."

Soooo what happens if the person deletes the files before restarting the computer? And also won't the stub run if he run the .exe file? :/

I'm not sure you understand what this exploit is exactly. I suggest googling, there is so much in the news about this. Do some research you will find your answers

galrov - February 24, 2019, 2:54 am

not sure what i am doing wrong but i make it and when i send it to VM antivirus detects it

Fisher - February 24, 2019, 3:32 am

(Feb 23, 2019 09:24 PM)?HOSTAH? Wrote: [\[CITE\]](#) CVE-2018-20250

exploit for Extracting Code Execution From Winrar

poc by Ridter

how to use ?

you just need to install python 3.7, and prepare a evil file you want to run, set the values you want, this exp script will generate the evil archive file automatically!

<https://github.com/WyAtu/CVE-2018-20250>

Enjoy. ? ?

Thanks man ! ? ? ? ?

Jacque Fresco - February 24, 2019, 4:57 am

Well it does not work with the latest release "WinRAR x64 (64 bit) 5.70 beta 2" Winrar just responds with "The Archive is either in unknown format or damaged"

Goldmouth - February 24, 2019, 6:04 am

(Feb 23, 2019 09:26 PM)#Skyline? Wrote: [\[CITE\]](#) Now this is useful. Thank you for the share. Thnx for the love ?

(Feb 24, 2019 12:01 AM)?????? Wrote: [\[CITE\]](#) yeap , thanks for the share it bro ...a good one! Happy spreading! Happy to help out. ?

(Feb 24, 2019 02:33 AM)Vakaris Wrote: [\[CITE\]](#) Thanks a lot! ?

(Feb 24, 2019 05:57 AM)Jacque Fresco Wrote: [\[CITE\]](#) Well it does not work with the latest release "WinRAR x64 (64 bit) 5.70 beta 2" Winrar just responds with "The Archive is either in unknown format or damaged"
Im sure they have patched some version of it.

Angelis - February 24, 2019, 6:05 am

I always liked you OP. Thanks for the share, I am sure a bunch of skiddos gonna wet their beds over this.

BTC - February 24, 2019, 6:32 am

(Feb 24, 2019 05:57 AM)Jacque Fresco Wrote: [\[CITE\]](#) Well it does not work with the latest release "WinRAR x64 (64 bit) 5.70 beta 2" Winrar just responds with "The Archive is either in unknown format or damaged"
yes the ace library has been removed since the release of the exploit to the public.

winrar is not setup to auto-install updates in any sort of way, the amount of computers with the new version patching the exploit is likely less than 0.01%. This leaves a huge amount of victims to blackhat users. Not that I agree with any such thing, but given the nature of the software this is a huge exploit to come out haha.

Jacque Fresco - February 24, 2019, 7:57 am

(Feb 24, 2019 07:04 AM)?HOSTAH? Wrote: [\[CITE\]](#) Im sure they have patched some version of it.
(Feb 24, 2019 07:32 AM)Apex Wrote: [\[CITE\]](#) yes the ace library has been removed since the release of the exploit to the public.

winrar is not setup to auto-install updates in any sort of way, the amount of computers with the new version patching the exploit is likely less than 0.01%. This leaves a huge amount of victims to blackhat users. Not that I agree with any such thing, but given the nature of the software this is a huge exploit to come out haha.

Good point @Apex

Well yeah that winrar does not update itself is a big neg. But i cant just agree with that less then 0.01% of computers running a exploitable winrar version (not want to explain myself yet). However Thanks for the Share @OP!

BTC - February 24, 2019, 8:08 am

(Feb 24, 2019 08:57 AM)Jacque Fresco Wrote: [\[CITE\]](#) Good point @Apex

Well yeah that winrar does not update itself is a big neg. But i cant just agree with that less then 0.01% of computers running a exploitable winrar version (not want to explain myself yet). However Thanks for the Share @OP!

Thanks bro ? its quite the opposite actually, less than 0.01% I estimate of machines with winrar installed, being actively used would be on the latest winrar update making them immune to this exploit.

MagicianMan32 - February 25, 2019, 3:28 am

Winrar is one of the most outdated softwares on most users' PCs
such an exploit will have a huge impact
thanks for sharing

Onireves - February 25, 2019, 3:40 am

Thanks for the share, going to try it out

R4NS0M - February 25, 2019, 3:51 am

I'm having problems with it. Could someone give me a hand?

blackbox99 - February 25, 2019, 4:49 am

i tried with some .jpg files and is not working, is unpacking the exe on desktop. I can use only .txt file to make it work?

killerila - February 25, 2019, 6:05 am

Nice! Thank you for sharing ?

BTC - February 25, 2019, 6:40 am

(Feb 25, 2019 05:49 AM)blackbox99 Wrote: [\[CITE\]](#) i tried with some .jpg files and is not working, is unpacking the exe on desktop. I can use only .txt file to make it work?

You need to target the decompression path of where you want the file to be.

I suggest doing somewhere that does not require administrative privileges to maximize compatibility across all versions of windows. The example used as the startup folder is most optimal, I personally use the "font" folder after a friend suggested to me, because who the fuck ever looks in there?

Fisher - February 25, 2019, 8:20 am

This exploit was patched on 5.61 winrar version as well.

BTC - February 25, 2019, 8:21 am

(Feb 25, 2019 09:20 AM)Trojanisches Pferd Wrote: [\[CITE\]](#) This exploit was patched on 5.61 winrar version as well.

No it wasn't. I've tested on all versions of 5.61.

Fisher - February 25, 2019, 8:30 am

(Feb 25, 2019 09:21 AM)Apex Wrote: [\[CITE\]](#) No it wasn't. I've tested on all versions of 5.61.

I have 5.61 version and i just tested its not working.

blackbox99 - February 25, 2019, 8:40 am

is working on 5.61, but the rar must be in "Downloads" folder when is extracted to work. What patch i must enter to work from every folder on computer?

retrax - February 25, 2019, 11:09 am

(Feb 25, 2019 07:40 AM)Apex Wrote: [\[CITE\]](#) You need to target the decompression path of where you want the file to be.

I suggest doing somewhere that does not require administrative privileges to maximize compatibility across all versions of windows. The example used as the startup folder is most optimal, I personally use the "font" folder after a friend suggested to me, because who the fuck ever looks in there?

Hi what path do you set for extraction ? i use this path

"C:\C:C:.\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\hi.exe" but when i try extracting it, it just blocks it from extracting into the startup directory ! Am using the 5.50 version by the way !

lol figured the path thing but bad news is Gmail and Other major email providers have already blocked RAR and other formats :D

Jacque Fresco - February 25, 2019, 12:04 pm

(Feb 25, 2019 09:21 AM)Apex Wrote: [\[CITE\]](#) No it wasn't. I've tested on all versions of 5.61.

(Feb 25, 2019 09:30 AM)Trojanisches Pferd Wrote: [\[CITE\]](#) I have 5.61 version and i just tested its not working.

Well ill tested that too with @WyAtu Github repo and from @Evi1cg. However it doesnt work with the 5.61 version. The archive can be opened, which is something that did not work with the 5.70 beta and yeah thats it. No hidden file deployment at all.

May someone with a older version of winrar can share it?

*****WOLF***** - February 25, 2019, 10:26 pm

I can confirm its work on 5.61 , not working on 5.71 beta2!

peterzoro - February 26, 2019, 4:13 am

it works on windows folders like desktop, downloads but not custom user created folders.

SIM-4062753 - February 26, 2019, 6:52 am

great idea dangerous vulnerability and a nice exploitation

Good helpful Post ?

raghavagarwal - February 26, 2019, 10:31 am

which tool i use to crack whatsapp and instagram

RATTAH - February 26, 2019, 1:20 pm

This is detected now and won't get you anything /thread

Goldmouth - February 26, 2019, 1:23 pm

(Feb 23, 2019 09:26 PM)#Skyline? Wrote: [\[CITE\]](#) Now this is useful. Thank you for the share.

(Feb 26, 2019 02:20 PM)RATTAH Wrote: [\[CITE\]](#) This is detected now and won't get you anything /thread

wtf are you talking about? this is working just fine.

galrov - February 26, 2019, 1:40 pm

its ur rat LOL

ur using shitty encryption

Zexture - February 26, 2019, 1:41 pm

Fucking hell....

<https://thehackernews.com/2019/02/winrar-hacking-exploit.html>

(Feb 26, 2019 02:40 PM)galrov Wrote: [\[CITE\]](#) its ur rat LOL

ur using shitty encryption

It's not from the OP. It's from the researcher who found the vulnerability. Also it's open source you can kinda figure out what's going on if you know a bit of python

galrov - February 26, 2019, 1:49 pm

(Feb 26, 2019 02:41 PM)Zexture Wrote: [\[CITE\]](#) Fucking hell....

<https://thehackernews.com/2019/02/winrar-hacking-exploit.html>

It's not from the OP. It's from the researcher who found the vulnerability. Also it's open source you can kinda figure out what's going on if you know a bit of python

ur retarded obviously nobody is that smart here to do that

Takehito Morokuzu - February 26, 2019, 3:14 pm

(Feb 26, 2019 02:23 PM)?HOSTAH? Wrote: [\[CITE\]](#) wtf are you talking about? this is working just fine.

It's not working for me. And I'm using WinRAR 5.5. The placeholder files extract fine but the calc is not extracted to the startup folder.

EDIT: It says the following file already exists: C:\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start-up\hi.exe

But when I check the folder it's not there...

Zexture - February 26, 2019, 3:15 pm

(Feb 26, 2019 02:49 PM)galrov Wrote: [\[CITE\]](#) ur retarded obviously nobody is that smart here to do that

you're*

No one here did that. A researcher found the vulnerability and posted an exploit for it. The OP just posted the link to his exploit

(Feb 26, 2019 04:14 PM)-yuno gasai- Wrote: [\[CITE\]](#) It's not working for me. And I'm using WinRAR 5.5. The placeholder files extract fine but the calc is not extracted to the startup folder.

It will be extracted to the folder above the current folder in AppData\.....

So if you extracted the file in Downloads\rrr\ The calc will be extracted Downloads\AppData\Roaming.....

Silent hill - February 26, 2019, 3:18 pm

(Feb 26, 2019 04:14 PM)-yuno gasai- Wrote: [\[CITE\]](#) It's not working for me. And I'm using WinRAR 5.5. The placeholder files extract fine but the calc is not extracted to the startup folder.

EDIT: It says the following file already exists: C:\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Start-up\hi.exe

But when I check the folder it's not there...

yeah same problem.

Takehito Morokuzu - February 26, 2019, 3:19 pm

(Feb 26, 2019 04:15 PM)Zexture Wrote: [\[CITE\]](#) you're*

No one here did that. A researcher found the vulnerability and posted an exploit for it. The OP just posted the link to his exploit

It will be extracted to the folder above the current folder in AppData\.....
So if you extracted the file in Downloads\rrr\ The calc will be extracted
Downloads\AppData\Roaming.....
Yeah I just figured that out. That's pretty useless TBH

NVM, most people will extract the file from their downloads folder, that's pretty smart, I'm tired lol I should've figured that out earlier

Zexture - February 26, 2019, 3:22 pm

(Feb 26, 2019 04:19 PM)-yuno gasai- Wrote: [\[CITE\]](#) Yeah I just figured that out. That's pretty useless TBH

Not really there are thousands including myself who will extract the file in their Downloads or Desktop. Also the exploit could be modified to change the page two directories above I'm not still sure though.

Takehito Morokuzu - February 26, 2019, 3:32 pm

(Feb 26, 2019 04:22 PM)Zexture Wrote: [\[CITE\]](#) Not really there are thousands including myself who will extract the file in their Downloads or Desktop. Also the exploit could be modified to change the page two directories above I'm not still sure though.

Yeah I'm tired but it makes sense now ?

This could be useful ?

galrov - February 26, 2019, 3:42 pm

how come its getting detected by defender now though

Takehito Morokuzu - February 26, 2019, 4:02 pm

(Feb 26, 2019 04:42 PM)galrov Wrote: [\[CITE\]](#) how come its getting detected by defender now though It isn't, I'm using defender right now and nothing was detected.

Fisher - February 26, 2019, 11:12 pm

(Feb 26, 2019 05:02 PM)-yuno gasai- Wrote: [\[CITE\]](#) It isn't, I'm using defender right now and nothing was detected.

Its detected for sure i thanked in beginning that is not detecting but it is.

GiraffeBear - February 26, 2019, 11:36 pm

Thanks. I can't believe that WinRAR had this exploit the whole time... Wonder how many people knew about this RCE for years.

Takehito Morokuzu - February 27, 2019, 1:04 am

(Feb 27, 2019 12:12 AM)Trojanisches Pferd Wrote: [\[CITE\]](#) Its detected for sure i thanked in beginning that is not detecting but it is.

I have defender on the latest Windows 10 and it is not detected. I can extract the archive, it extracts the malicious payload and my antivirus sits there watching the whole thing.

peterzoro - February 27, 2019, 3:20 am

avast detecting on scan time now.

Joaquillio - February 27, 2019, 12:51 pm

(Feb 24, 2019 03:54 AM)galrov Wrote: [\[CITE\]](#) not sure what i am doing wrong but i make it and when i send it to VM antivirus detects it
Deactivate it.

smau - February 28, 2019, 1:54 am

(Feb 23, 2019 09:24 PM)?HOSTAH? Wrote: [\[CITE\]](#) CVE-2018-20250

exploit for Extracting Code Execution From Winrar

poc by Ridter

how to use ?

you just need to install python 3.7, and prepare a evil file you want to run, set the values you want, this exp script will generate the evil archive file automatically!

<https://github.com/WyAtu/CVE-2018-20250>

Enjoy. ? ?
great man

tempm100 - March 7, 2019, 9:23 pm

```
[*] Start to generate the archive file test.rar...
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
[+] Evil archive file test.rar generated successfully !
```

what im doing wrong ?

galrov - March 7, 2019, 9:31 pm

nothing thats how its supposed to be

tempm100 - March 7, 2019, 9:32 pm

you sure? its not wroking then..

ucplusx - March 7, 2019, 10:53 pm

```
(Mar 7, 2019 10:23 PM)tempm100 Wrote: \[CITE\] [*] Start to generate the archive file test.rar...
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
[+] Evil archive file test.rar generated successfully !
```

what im doing wrong ?have you test your .exe before exploit it into rar?
if your exe fud already and works good after,so maybe your rar programs was being corructed by AV

G0dzSoldiers - April 2, 2019, 5:20 pm

Thanks for sharing this my guy OP

wrapmycode - April 4, 2019, 12:34 am

thank you bro, I have to test it.

f-Hacking_ph - October 6, 2019, 2:29 pm

Thank you for sharing FREE! (and not take advantage of the circumstance...)
Regards.

