

CVE-2020-36241: A malicious archive allows Directory Traversal during extraction

Original reporter: [Yigit](#)

Area: Application

Message

Summary: A malicious package may be able to overwrite arbitrary files

Proof of concept: 1- Download "example.tar" 2- Click on the right button on a mouse (on "example.tar") 3- Click "Extract Here" 4- Check the "/tmp" path for "test" file

Version: Ubuntu 20.04.1 GNOME Files 3.36.3-stable

Note: This report created on <https://security.gnome.org/>, I can't add proof of concept video and file.

Edited 1 year ago by [Ondrej Holy](#)

📁 Drag your designs here or [click to upload](#)

Tasks 📌 0


No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 🔗 0


Related merge requests 🔗 1

[doap: Update maintainers](#)
110


Activity

**Michael Catanzaro** @mcatanzaro · 2 years ago Developer


Hi, thanks for your report. Can you give us a URL to your example.tar, please?
You could also try attaching it to your reply, although I'm not entirely sure whether that will work or not.

**GitLab Support Bot** @support-bot · 2 years ago Author


Hello, Thank you for your response.
Proof of concept file (example.tar) : <https://we.tl/YO9abvVF8e> Proof of concept video (test.mp4) : <https://we.tl/qLcWfMac9w>
Thank you,
Michael Catanzaro gitlab-issues@gnome.org, 6 Kas 2020 Cum, 19:23 tarihinde şunu yazdı:

**António Fernandes** @antoniof · 1 year ago Developer


The download link has expired. Has anyone downloaded it who can attach it to the issue?

**Ondrej Holy** @oholy · 1 year ago Maintainer


Dammit, I probably removed that archive by mistake from my drive and I don't know how to create it easily.
Edited by [Ondrej Holy](#) 1 year ago

**Ondrej Holy** @oholy · 1 year ago Maintainer

It contained a symlink which points outside of the archive (this is ok). But then it contains a file that has the symlink in its path (which is not ok), so it means that it will be extracted outside of the destination...


**Ondrej Holy** @oholy · 1 year ago Maintainer

[@yigitcnyilmaz046](#) Can you please reupload it for testing purposes?


**Ondrej Holy** @oholy · 1 year ago Maintainer

I have finally found a way how to create such an archive - [@linktotmp.tar](#) (it contains `tmpLink` symlink which points to `/tmp` and `tmpLink/foo` file).


Please [register](#) or [sign in](#) to reply

**Michael Catanzaro** @mcatanzaro · 2 years ago Developer


This looks very similar to file-roller CVE-2020-11736, [file-roller@21dfc@v](#). Looks like it was fixed only at the file-roller level, but a solution in libarchive itself is required or everything else that uses libarchive is still vulnerable. CC [@oholy](#)
We will need a new CVE request as well.


**GitLab Support Bot** @support-bot · 2 years ago Author

Hello, Can you share last situation with me ? Also, can you share URL for follow this report?
Thank you,
Michael Catanzaro gitlab-issues@gnome.org, 6 Kas 2020 Cum, 20:45 tarihinde şunu yazdı:


**Michael Catanzaro** @mcatanzaro · 2 years ago Developer

Hi, there have been no further updates on this issue. It requires further investigation by the nautilus maintainers.
This issue is <https://gitlab.gnome.org/Teams/Releng/Security/-/issues/6>, but to view that URL you would need an account on GNOME GitLab. Then I would need to CC your account on the issue. If you want to create an account, let me know what your username is and I can CC you.


**Michael Catanzaro** changed title from (-Service Desk (from yigitcnyilmaz@gmail.com): New Security Issue-) to A malicious archive may be able to overwrite arbitrary files 2 years ago

**Michael Catanzaro** @mcatanzaro · 2 years ago Developer


After this has been investigated, we will probably need to request a new CVE using <https://cveform.mitre.org/>. Whether for nautilus or for libarchive, I'm not sure.

**GitLab Support Bot** @support-bot · 2 years ago Author


Hello, Please add me as CC to report. My username is yigitcnyilmaz046
Thank you,
Michael Catanzaro gitlab-issues@gnome.org, 11 Kas 2020 Çar, 19:32 tarihinde şunu yazdı:

**Michael Catanzaro** @mcatanzaro · 2 years ago Developer


CC [@yigitcnyilmaz046](#)

**GitLab Support Bot** @support-bot · 2 years ago Author

Hello, I couldn't access to report with <https://gitlab.gnome.org/GNOME/nautilus/-/issues/1671> URL.
Thank you,
Michael Catanzaro gitlab-issues@gnome.org, 11 Kas 2020 Çar, 20:19 tarihinde şunu yazdı:

**Michael Catanzaro** @mcatanzaro · 2 years ago Developer

Hm, I'm surprised that didn't work.
You should still be receiving emails for all updates, however, so hopefully that will suffice...




GitLab Support Bot @support-bot · 2 years ago

Author

Hello, I have not received any updates (excluding your e-mails).

Thank you,


Michael Catanzaro gitlab-issues@gnome.org, 11 Kas 2020 Çar, 20:43 tarihinde şunu yazdı:



Michael Catanzaro @mcatanzaro · 2 years ago

Developer

You should be receiving an email for every comment in this issue. So far, nobody else has replied to this issue except for me, so it's expected that you haven't received other emails yet.




Ondrej Holy @oholy · 2 years ago


Maintainer

Although I was added to this issue 5 days ago, I have got a notification a few hours ago, so the GitLab notifications seem to be broken somehow. I will try to look at this soon. But if I am not mistaken, libarchive just provides a low-level API to read archives, it doesn't write anything. Thus I think that this is rather a bug in Nautilus or gnome-autor and we need something like the mentioned file-roller fix. But maybe there is something which can be done on libarchive side. Just note that GVfsBackendArchive also uses libarchive, but it doesn't follow symlinks at all for this reason...

/cc [@antoniof](#)




Ondrej Holy added [1 Bug](#), [1 Security](#), [5 Archives handling in Files](#) labels 2 years ago



Ondrej Holy @oholy · 2 years ago

Maintainer


I went thru the codes and found that this is actually gnome-autor bug. Just note that libarchive has its extractor which accepts ARCHIVE_EXTRACT_SECURE_SYMLINKS flag presumably for this reason, however, gnome-autor implements extraction in its own way. So I would say that there is not much what libarchive could do better in this case except for some warning in the documentation. I have prototyped a potential fix for it: [18 AutoarExtractor-Do-not-extract-files-outside-the-des.patch](#). I am attaching it here as there is no way to create private MR if I am not mistaken. Is somebody willing to check that?



António Fernandes @antoniof · 1 year ago

Developer

Patch looks good to me, diff-wise. I'm to applying and testing it now.




Ondrej Holy @oholy · 1 year ago

Maintainer

Thanks for feedback

Please [register](#) or [sign in](#) to reply




GitLab Support Bot @support-bot · 2 years ago

Author

Hello Ondrej, Can you add me to report as CC ? My username is yigiticanyilmaz046

Thank you,

Ondrej Holy gitlab-issues@gnome.org, 16 Kas 2020 Pzt, 18:47 tarihinde şunu yazdı:




Michael Catanzaro @mcatanzaro · 2 years ago

Developer

You're already CCed on this report.

I'm not sure why you can't see it directly on the web, but the new URL is: [#7 \(closed\)](#).



GitLab Support Bot @support-bot · 2 years ago

Author


Hello, I can't access. If I enter the this URL, I see "404 Page Not Found"

Can you add me as /cc yigiticanyilmaz046 ?

/cc yigiticanyilmaz046

Thank you,


Michael Catanzaro gitlab-issues@gnome.org, 16 Kas 2020 Pzt, 19:57 tarihinde şunu yazdı:



Michael Catanzaro @mcatanzaro · 2 years ago

Developer

You are already CCed, so I don't think there's anything else we can do to give you access, sorry.




GitLab Support Bot @support-bot · 2 years ago

Author

Hello, OK. Thank you. After fix this issue, can anyone access this report ?

Thank you,


Michael Catanzaro gitlab-issues@gnome.org, 16 Kas 2020 Pzt, 20:22 tarihinde şunu yazdı:



Michael Catanzaro @mcatanzaro · 2 years ago

Developer

Yes, we should remember to make this issue public once it is fixed.



GitLab Support Bot @support-bot · 2 years ago


Author

Hello Michael, Also, I reported a new security issue. Please set it as confidential. I can't do this.

<https://gitlab.gnome.org/Teams/Releng/security/-/issues/7>

Thank you,

Michael Catanzaro gitlab-issues@gnome.org, 16 Kas 2020 Pzt, 20:35 tarihinde şunu yazdı:



GitLab Support Bot @support-bot · 2 years ago


Author

Hello, I reported a new security issue. Please set it as confidential. I couldn't do this.

Report : <https://gitlab.gnome.org/Teams/Releng/security/-/issues/7>

Thank you,

Yigit Can Yilmaz yigiticanyilmaz@gmail.com, 16 Kas 2020 Pzt, 19:38 tarihinde şunu yazdı:




Bastien Nocera @hadess · 2 years ago

Developer

This looks very similar to file-roller CVE-2020-11736, [File-roller@214fcdbf](#). Looks like it was fixed only at the file-roller level, but a solution in libarchive itself is required or everything else that uses libarchive is still vulnerable. CC [@oholy](#)

FYI, I checked the evince comics backend, and it shouldn't be impacted by this misfeature, as it doesn't actually extract any files to disk.




GitLab Support Bot @support-bot · 2 years ago

Author

Hello, I want to learn situation.

Thank you,

19 Kas 2020 Per, saat 14:52 tarihinde Bastien Nocera < gitlab-issues@gnome.org > şunu yazdı:




Michael Catanzaro @mcatanzaro · 2 years ago

Developer

Hi, there are no further updates on this issue. You're already receiving emails for all updates.


[@lantw](#) [@csoriano](#), you are listed as maintainers for gnome-autor. Please acknowledge, thanks!



Ondrej Holy @oholy · 2 years ago

Maintainer


Unfortunately, I am afraid that we won't get any reaction from them after looking at their GitLab activity in the last months. Perhaps [@felipeborges](#) could double-check that?



Ondrej Holy @oholy · 1 year ago

Maintainer

Or [@antoniof](#) could double-check?




Ondrej Holy @oholy · 1 year ago

Maintainer

Just note that I will probably take over gnome-autor maintainership, see [110 \(merged\)](#).


Please [register](#) or [sign in](#) to reply

**Michael Catanzaro** @mcatanzaro · 1 year ago Developer

Please note this vulnerability will be made public this Thursday (90 days after original report).

I am attaching it here as there is no way to create private MR if I am not mistaken.

There is a Create Confidential Merge Request button at the top of this issue. It's to the right of the up/down thumbs, then there is the emoji button. Oldest first. Show all activity. Create confidential merge request.

**Ondrej Holy** @oholy · 1 year ago Maintainer

Hmm, so it is probably a good time to merge that fix. I see that button, so I created gnome-autoar fork, but I am not able to set the project visibility to private.

Project visibility ⓘ


Public

Private


Internal

Public


Edited by **Ondrej Holy** 1 year ago

**Ondrej Holy** @oholy · 1 year ago Maintainer

I've just opened issue for it: <https://gitlab.gnome.org/Infrastructure/Infrastructure/-/issues/519>


**Ondrej Holy** @oholy · 1 year ago Maintainer

Created https://gitlab.gnome.org/oholy/gnome-autoar/-/merge_requests/1.


**António Fernandes** @antoniof · 1 year ago Developer

I can't access the MR. "404 Page Not Found"

Edited by **António Fernandes** 1 year ago


**Bartłomiej Piotrowski** @barthalion · 1 year ago Owner

It seems to be a merge request against Ondrej's fork itself and not the original repo.

**Ondrej Holy** @oholy · 1 year ago Maintainer


It can't be against the original repo as it won't be confidential MR, or I don't understand how that should work. I have just added **@antoniof** as a member of the fork, so he should have access now...

Edited by **Ondrej Holy** 1 year ago

**Bartłomiej Piotrowski** @barthalion · 1 year ago Owner


Ah, my bad, I was reading documentation for the next GitLab release... yeah, seems there's no other way than this at the moment.

Please [register](#) or [sign in](#) to reply


**Ondrej Holy** @oholy · 1 year ago Maintainer

Please note this vulnerability will be made public this Thursday (90 days after the original report).

@mcatanzaro, what does this mean exactly? That somebody will file CVE for it, who? Is something else expected from me (as a new gnome-autoar maintainer) apart from fixing it?

**Ondrej Holy** @oholy · 1 year ago Maintainer

@mcatanzaro, **@antoniof** likes the fix, so may I merge it now, or is there some special workflow for it?

**Michael Catanzaro** @mcatanzaro · 1 year ago Developer

what does this mean exactly?


It means I'll toggle the confidentiality status. But since you're about to merge the fix, you could do that now yourself.

That somebody will file CVE for it, who?

If you're going to be maintaining gnome-autoar, I recommend applying for the CVE yourself using <https://cveform.mitre.org/>. Alternatively, the reporter could do so.

Is something else expected from me (as a new gnome-autoar maintainer) apart from fixing it?

Nope. Bonus points if you request a CVE, though, as otherwise stable distros will not fix this.

**Ondrej Holy** @oholy · 1 year ago Maintainer

So I've just merged the fix, toggled the confidentiality status, and going to request CVE.

Please [register](#) or [sign in](#) to reply

**GitLab Support Bot** @support-bot · 1 year ago Author

Hello Michael, Can you give me CVE for this issue ?

Thank you,

Michael Catanzaro gitlab-issues@gnome.org, 3 Şub 2021 Çar, 19:11 tarihinde şunu yazdı:

**Ondrej Holy** @oholy · 1 year ago Maintainer

I've requested CVE but the number is not assigned yet.

**Ondrej Holy** @oholy · 1 year ago Maintainer


CVE-2020-36241 has been assigned for this.

Edited by **Ondrej Holy** 1 year ago

Please [register](#) or [sign in](#) to reply

Ondrej Holy closed via commit [cd867e6](#) 1 year ago

Ondrej Holy made the issue visible to everyone 1 year ago

**Ondrej Holy** @oholy · 1 year ago Maintainer

I've just found that gnome-extensions binary provided by gnome-shell project, which also uses gnome-autoar library, seems to be affected by this as well...

Ondrej Holy changed title from A malicious archive may be able to overwrite arbitrary files to CVE-2020-36241: A malicious archive allows Directory Traversal during extraction 1 year ago

Ondrej Holy mentioned in issue [Infrastructure/Infrastructure#572 \(closed\)](#) 1 year ago

Please [register](#) or [sign in](#) to reply