Unrestricted File Upload Allowed due to Flawed Move File Functionality in octoprint/octoprint

0

Valid Reported on Aug 15th 2022

Description

Hello Team,
Hope you are doing good.
Due to misconfiguration in move file functionality an attacker could easily change the file extension of the uploaded malicious file disguised as .gcode file.

Steps:

1 . Upload a .gcode file & intercept the request as shown in the screenshots.
2 . Add malicious payload in the file content & keep file extension as .gcode.
3 . Now select the file & click on move button.
4 . Change the file extension to the html as shown in the screenshot & send the request.
5 . Copy the file download link & share it with the victim user. Once the file is opened payload will be executed.

Image POC

https://drive.google.com/drive/folders/1cbbJKiOqZdgIbGM3Bx09Xq6Xjkkje948?usp=sharing

Impact

Using this technique an attacker could trick a victim user in downloading a malicious file such as virus, html file containing cross site scripting payloads, etc.

Occurrences

files.py L1-L1312

CVE

CVE
CVE-2022-2872
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Low (3.7)

Registry
Pypi

Affected Version
1.8.2

Visibility
Public

Status
Fixed

Found by

Gaurish Kauthankar
@argonx21
unranked

Fixed by

Gina Häußge
@foosel
maintainer

This report was seen 894 times.

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

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

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

Gina Häußge 3 months ago

I arrive at a CVSS vector string of CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N and thus a score of 3.7 (Low) for this.

My reasoning:

AV:N - network attack vector
AC:H - an attacker needs to get access to an instance with rights to upload AND move, or talk someone else into doing this for them. Then they need to further target another user of the instance and talk them into going to a download URL of an uploaded file in their browser. Given that OctoPrint is supposed to be run in trusted LANs instead of the internet, for this to succeed an attacker either needs collaboration from the victim by misconfiguration in shape of blind port forwarding, or another successful attack (possibly social in nature) to get access to the network and thus the instance in the first place.
PR:L - no attack without an account on the instance, or a severe misconfiguration of the instance
UI:R - the victim needs to collaborate to execute the attack
S:U - no credentials can be stolen via XSS as they are all http only
C:L - the attacker might be able to run commands as the victim, but only to the limit of their account restrictions
I:L - the attacker might be able to run commands as the victim, but only to the limit of their account restrictions
A:N - no loss of availability

Gina Häußge modified the Severity from Medium (6.5) to Low (3.7) 3 months ago

Gina Häußge assigned a CVE to this report 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

Gaurish Kauthankar has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Gaurish 3 months ago Researcher

Thanks Gina

Gina Häußge 3 months ago Maintainer

Fix is forthcoming in 1.8.3. It's already done, just compiling a slightly more encompassing security/bugfix release first before pushing that publicly.

Gaurish 3 months ago Researcher

Hi Gina, let me know once the cve is published in nist.

Thanks.

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

Gaurish 3 months ago Researcher

Any update on cve?

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

Charlie Powell 3 months ago Maintainer

@Researcher the fix is in private testing and will be released in good time. OctoPrint's security policy does ask for a 90 day disclosure window, so please be patient while everything is sorted out properly.

Gaurish 3 months ago Researcher

Thank you for the update.

We have sent a third and final fix follow up to the **octoprint** team. This report is now considered stale. 3 months ago

Gina Häußge marked this as fixed in **1.8.3** with commit **3e3c11** 2 months ago

Gina Häußge has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

files.py#L1-L1312 has been validated ✔

Gaurish 2 months ago Researcher

Hi Gina, can you please help me with the cve registration?. I still can't any update on the nist website regarding my cve.

Gina Häußge 2 months ago Maintainer

Out of my jurisdiction, something for @admin.

Jamie Slome 2 months ago Admin

The CVE has been published here 👍

@Gaurish - please feel free to get in touch with us directly if you have any more questions about a CVE.

Gaurish 2 months ago Researcher

Thanks for the update @Jaime.. Have a great day !

Sign in to join this conversation