huntr

Cross-site Scripting (XSS) - Generic in octoprint/octoprint

0

✓ Valid Reported on Apr 20th 2022

Description

The Stream URL of octoprint application allowing xss payload to execute for which its leads to Cross-site Scripting (XSS

Proof of Concept

Login to the application
Now go to settings -> Webcam & Timelapse -> Stream URL and insert the payload `"<img src=1 onerror=alert(document.cookie)>` in the Stream URL and click on "Test"
You will see that its making a internal GET request

Image POC

```
https://drive.google.com/drive/folders/1gvRKz8AKOY8XE3O3z4mJdr61heIxGtH7?us
```

Impact

User accounts can be hijacked, credentials could be stolen, sensitive data could be exfiltrated, and lastly, access to your client computers can be obtained.

CVE
CVE-2022-1432
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Generic

Severity
High (7.5)

Registry
Other

Affected Version
1.7.3

Visibility
Public

Status
Fixed

Found by

Raj
@rajbabai8
master

Fixed by

Gina Häußge
@foosel
maintainer

This report was seen 677 times.

We are processing your report and will contact the **octoprint** team within 24 hours. 7 months ago

Raj modified the report 7 months ago

A **octoprint/octoprint** maintainer has acknowledged this report 7 months ago

Raj modified the report 7 months ago

We have contacted a member of the **octoprint** team and are waiting to hear back 7 months ago

Gina Häußge 7 months ago

As being able to successfully launch this attack would require the attacker to a
admin rights (as that is required to modify the mentioned URL), I do not agre
"critical" here.

I'd actually lean towards "none" (it is kind of a senseless thing to run this attack if you already have full admin rights on the instance anyhow), but would be willing to compromise on "low" considering that 3rd party clients might be compromised with a manipulated URL (though in that case it would also require a lack of sanitisation on their end).

Gina Häußge modified the report 7 months ago

Gina Häußge modified the report 7 months ago

Gina Häußge modified the report 7 months ago

Gina Häußge validated this vulnerability 7 months ago

Read through the CVSS docs and now classified as CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H, so high severity.

An attacker would need network access to a target instance, find a user that already has admin rights, somehow talk them into replacing the webcam URL with something completely broken (there's no easy way to do this with a prepared link or something like with the login xss issue, and usually no motivation to do so either) before being able to successfully execute this attack - that requires a ton of work with uncertain outcome. No scope change.

Will look into fixing this, thanks for finding it.

Raj has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Raj 7 months ago Researcher

@admin As the severity is high 7.5 why I haven't received the bounty for this report?

Jamie Slome 7 months ago Admin

Sorted for you 👍

We have sent a fix follow up to the **octoprint** team. We will try again in 7 day

Chat with us

We have sent a second fix follow up to the **octoprint** team. We will try again in 10 days. 7 months ago

We have sent a third and final fix follow up to the **octoprint** team. This report is now considered stale. 6 months ago

Gina Häußge 6 months ago

A fix has been prepared and will be rolled out with 1.8.0, which is planned to be released next week.

Jamie Slome 6 months ago Admin

Thanks for the update @Gina. Once the fix has been rolled out, feel free to update the report with the commit SHA which addresses the issue 👍

Gina Häußge 6 months ago

@admin That is the plan, however it's currently not available in a public repository due to still being under review and testing by myself and some trusted people, and thus I couldn't do that yet (and a public repo is out of the question until just before release to not put people at risk). Your rather insistent automated emails prompted me to at least comment that this was well underway ;)

A friendly suggestion, would it be possible to add some option to mark this as "in progress" in the future? IMHO there's definitely a state between "awaiting fix" and "fixed and can go public right away"

Jamie Slome 6 months ago Admin

@Gina - thanks for the info on this. I think there are definitely opportunities for improvement here.

I definitely agree that some "in progress" option is required, allowing maintainers to halt further e-mail notifications (as we definitely don't want to bug you) and let the researcher know that a fix is on the way, but might take a bit of time.

How does this sound? Would you mind if I added the above feedback to our public discussion here, just so we can stay on top of it? I will remove your username and any identifying information before doing so :)

Chat with us

Gina Häußge 6 months ago

@admin sure, go ahead! I'm in the middle of prepping lunch or I'd do it myself even 😅 No need to anonymise me, feel free to even tag me (@foosel on GitHub)

Gina Häußge 6 months ago

I should add, no need to to anonymise me, but keep the issue out of it - that still needs to stay private until I've been able to push out the 1.8.0 release.

Jamie Slome 6 months ago Admin

Amazing 🤝 I've posted a comment on the discussion here.

Enjoy your lunch 🥙

Raj 6 months ago Researcher

No worries you can take your time @Maintainer

Gina Häußge marked this as fixed in 1.8.0 with commit 6d259d 6 months ago

Gina Häußge has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us