huntr

Dom xss leads to account takeover in octoprint/octoprint

0

✓ Valid Reported on Apr 19th 2022

Description

The endpoint of login allows Javascript payload to execute which leads to XSS pop-up

Proof of Concept

Send this link to admin `http://127.0.0.1:2222/login/?redirect=javascript:alert(document.cookie)`
When he will open it and try to login XSS will popup.

Image POC

```
https://drive.google.com/file/d/1VoO0BHUE03o0iOo8B9WFRvC1zRrFN4-T/view?usp=
```

Impact

Attacker able to capture admin cookie and can takeover his account.

CVE
CVE-2022-1430
(Published)

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

Severity
High (7.5)

Registry
Pypi

Affected Version

Affected Version
1.7.3

Visibility
Public

Status
Fixed

Found by

Raj
@rajbabai8
master ⌄

Fixed by

Gina Häußge
@foosel
maintainer

This report was seen 737 times.

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

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

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

Gina Häußge modified the report 7 months ago

Gina Häußge validated this vulnerability 7 months ago

I have downgraded the severity to high. A scope change is not possible here, and a successful attack requires knowledge about the target system and preparation (you need not only get network access to a normally LAN only application but then also need to figure out who is an admin or has an account there for targeting with a prepared link that will then give you access to credentials via the vulnerability) and is the complexity therefore cannot be classified as "low" either.

Chat with us

Apart from that, thank you for finding this, because this is definitely a serious issue that needs fixing ASAP.

fixing ASAP.

Raj has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Gina Häußge 7 months ago

Maintainer

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

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

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

Maintainer

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

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 **808752** 6 months ago

Gina Häußge has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation