Insufficient Session Expiration in octoprint/octoprint

0

Valid Reported on Aug 16th 2022

Description

Insufficient Session Expiration is when a website permits an attacker to reuse old session credentials or session IDs for authorization.

Proof of Concept

```
Steps to reproduce
1- Login into http://127.0.0.1:5000/login/ (OctoPrint).
2- Open browser in the incognito tab or open another browser and login with
3- In step 1 change the password and login again.
4- In step 2 the old session is still valid, it must expire.
```

Impact

An attacker can use old session credentials or session IDs for authorization.

Occurrences

__init__.py L298

not sure of correct location

References

- cwe.mitre.org

CVE
CVE-2022-2888
(Published)

Vulnerability Type
CWE-613: Insufficient Session Expiration

Severity
Medium (4.4)

Registry
Pypi

Affected Version
<=1.8.2

Visibility
Public

Status
Fixed

Found by

Abdullah Baghuth
@0xcybery
amateur

Fixed by

Gina Häußge
@foosel
maintainer

This report was seen 799 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 modified the Severity from High (8.2) to Medium (4.4) 3 month

Gina Häußge 3 months ago Maintainer

After putting this through the CVSS calculator myself, I arrive at a vector string of CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N and thus a score of 4.4 (Medium)

Reasoning:

AV:L - you require access to the session cookie, which is stored in the victim's browser. That usually means you need local access. Any kind of secondary attacks to obtain the cookie remotely are not part of this particular vulnerability and thus don't factor into the scoring.
AC:L - IF you already have access to the cookie because you have access to the victim's browser session, then yes, this is low complexity
PR:L - however, you do need at the very least the victim's rights to access to cookie
UI:N - you don't need further assistance from the victim to make use of it
S:U - only OctoPrint affected
C:L - only the victim's OctoPrint account affected
I:L - only the victim's OctoPrint account affected
A:N - no impact on OctoPrint's availability

Gina Häußge 3 months ago Maintainer

@Administrator I'd like to validate this report, but change the summary that will be part of the CVE. As soon as I try to change that text however, the "Mark valid" button gets disabled. I'd like to change the description to this:

"If an attacker comes into the possession of a victim's OctoPrint session cookie through whatever means, the attacker can use this cookie to authenticate as long as the victim's account exists."

@Reporter I'll validate this as soon as the above problem is clarified. I can confirm this vulnerability, and it is an inherent problem with this kind of session management and something that likely affects more applications that use the same software stack. I have a fix in the pipeline that will ensure both the remember me token and the session cookie to be tied to the user's passwords (so changing those will invalidate the cookies automatically), and also changes the session handling inside OctoPrint to have sessions invalidate after 15min of inactivity. That requires some changes to the user experience, but that compromise should be bearable by the general audience. Combined with the fact that OctoPrint is meant to be run in a friendly LAN and not exposed to the public internet, that should suffice to mitigate this. Fix will be part of the forthcoming version 1.8.3.

Jamie Slome 3 months ago Admin

Hi @Gina, we are taking a look into this bug this morning and should have it r
We will keep you posted here 👍

Jamie Slome 3 months ago Admin

@Gina - as not to hold this up, feel free to proceed with marking this report as valid etc. I will adjust the CVE once it gets generated with the description you have suggested 👍

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

Gina Häußge validated this vulnerability 3 months ago

Abdullah Baghuth has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Gina Häußge 3 months ago Maintainer

@Admin Done! Can you also please adjust the Affected Version to <=1.8.2?

Jamie Slome 3 months ago Admin

Both sorted for you :) Once the fix has been confirmed in the UI, the CVE will be published with your elected description 👍

Gina Häußge 3 months ago Maintainer

Thank you very much!

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. 3 months ago

Gina Häußge marked this as fixed in **1.8.3** with commit **40e621** 2 months ago

Gina Häußge has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

__init__.py#L298 has been validated ✔

Sign in to join this conversation