Weak Password Change Mechanism in octoprint/octoprint

1

✓ Valid Reported on Aug 20th 2022

Description

The user password change page, doesn't require knowledge of the existing password.

Proof of Concept

Log in as a normal user
Go to the User Dashboard page and click `User Settings` .
Set a any new password.
Click `confirm`
The password is changed successfully.

Impact

An attacker that gains access to an active user session, can change the account password without previous knowledge of the current password.

CVE
CVE-2022-2930
(Published)

Vulnerability Type
CWE-620: Unverified Password Change

Severity
Medium (5.3)

Registry
Pypi

Affected Version
1.8.2

Visibility
Public

Status

Fixed

Found by

0xbeven

@bevennyamande

noisy

Fixed by

Gina Häußge

@foosel

maintainer

This report was seen 639 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

Gina Häußge modified the Severity from High (7.6) to Medium (4.4) 3 months ago

Gina Häußge modified the Severity from Medium (4.4) to Medium (5.3) 3 months ago

Gina Häußge 3 months ago Maintainer

I arrive at CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L for this and thus 5.3 (Medium)

AV:L - "Log in as a normal user". So you need access to the victim's browser session in the first place, and thus this is local.
AC:L - Once you have a login session, this is indeed low complexity
PR:L - You need to be able to use the victim's browser in their name, with regular privileges of them
UI:N - No further help from the user needed
S:U - Only OctoPrint is affected
C:L - Only the victim's account is affected
I:L - Only the victim's account is affected
A:L - Only the victim's account is affected

Chat with us

Ironically I already noticed this myself last week and fixed it on the development branch. So it'll be solved in 1.9.0 and actually 1.8.3 since I'll backport it to the next bugfix/security release.

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

Gina Häußge validated this vulnerability 3 months ago

0xbeven has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Gina Häußge marked this as fixed in **1.8.3** with commit **145307** 3 months ago

Gina Häußge has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

0xbeven 3 months ago Researcher

Thank you for this I will continue to test

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

FAQ

contact us

terms

privacy policy

Chat with us