huntr

# No rate limit on main Login page lead to account takeover in octoprint/octoprint

3

✓ Valid Reported on Aug 12th 2022

Hi Team,
Summary:
As a best practice a login page should have a rate limit to avoid any kind of brute force.
Aslo The password policy used in the account creation and password change pages is weak, allowing to set a password of only 1 character.

## Impact

An attacker can freely brute force username and password and can takeover any account. An attacker could easily guess user passwords and gain access to user and administrative accounts.

CVE
CVE-2022-2822
(Published)

Vulnerability Type
CWE-307: Improper Restriction of Excessive Authentication Attempts

Severity
Low

Registry
Other

Affected Version
<= 1.7.3

Visibility
Public

Status
Fixed

Found by

maakthon

@maakthon

amateur

Fixed by

Gina Häußge

@foosel

maintainer

This report was seen 738 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

**maakthon** modified the report 3 months ago

Gina Häußge 3 months ago Maintainer

Considering that OctoPrint is used to run consumer grade 3d printers and hence usually runs in a restricted LAN, unless the user has actively decided to make it accessible through a port forward or any other such configuration against all of OctoPrint's recommendations an attack like this would require significant work by the attacker to even obtain access to the instance in the first place, after learning it even is available. I'm therefore arriving at a CVSS vector string of CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N here, which boils down to a score of 3.7 and thus Low severity.

To further elaborate my classification:

AV:N - network access indeed suffices
AC:H - the attacker needs access to the network first, and knowledge of there being a target to exploit, as OctoPrint is usually not run on the public internet, not supposed to be run there, and frankly it doesn't even make sense to run it there either given that it needs physical connection to a 3d printer to even operate. The attacker also needs to brute force not only the password but also the username, and OctoPrint doesn't distinguish whether a failing attempt to login is due to a username or password mismatch.
PR:N - indeed no privileges required
UI:N - no user interaction required
S:U - the only victim in case of a successful attack is OctoPrint
C:L - the brute forced user account gets taken over, nothing else
I:N - no side effects on the integrity of the system

A:N - no side effects on the availability of the system

Even if we assume AC:L (which given the mode of operation of OctoPrint is a long stretch here) we arrive at a score of 5.3 (Medium).

I'm therefore downgrading the severity of this report.

**Gina Häußge** modified the Severity from High to Low 3 months ago

**Gina Häußge** modified the CWE from Authentication Bypass by Primary Weakness to Improper Restriction of Excessive Authentication Attempts 3 months ago

Gina Häußge 3 months ago Maintainer

I've also just noticed that the selected CWE wasn't the right one, CWE-307 Improper Restriction of Excessive Authentication Attempts is *precisely* what this is about from my understanding, so I've changed that as well.

**Gina Häußge** assigned a CVE to this report 3 months ago

The researcher has received a minor penalty to their credibility for misclassifying the vulnerability type: -1

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

**Gina Häußge** validated this vulnerability 3 months ago

**maakthon** 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 **1.9.0** with commit **82c892** 3 months ago

**Gina Häußge** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

maakthon 3 months ago

Chat with us

Thank you so much for these valuable information.
Also appreciate for assign CVE.
Thanks.

Gina Häußge 3 months ago Maintainer

You are welcome!

Gina Häußge 3 months ago Maintainer

@admin I was sure I had provided a slightly more explanatory description when requesting the CVE assignment, but on the published CVE now I still only see the somewhat generic text that originates from the Impact here. Did I do something wrong or is there some underlying workflow issue here?

Jamie Slome 3 months ago Admin

Hi Gina, apologies for this. It looks like a bug from our side. Ben from our team is looking into what happened here and we will keep you updated.

Gina Häußge 3 months ago Maintainer

Hi Jamie, thank you, good to know it's apparently not my fault then 😅

Jamie Slome 3 months ago Admin

Not at all!

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