Privilage escalation allows user with read access only to edit admin portal and take actions in octoprint/octoprint

1

Valid Reported on Aug 23rd 2022

Overview of the Vulnerability

Authentication and session management controls can be bypassed in a variety of ways including, calling an internal post-authentication page, modifying the given URL parameters, by manipulating the form, or by counterfeiting sessions. The authentication method for this application can be bypassed by an attacker which enables them to access a privileged user's account and functionality, giving them access to more resources or functionality within the application. This could include viewing or editing sensitive customer data, and viewing or editing other user permissions.

Business Impact

The impact of privilege escalation through broken authentication controls can vary in severity depending on the degree of access to resources or functionality the malicious attacker is able to gain. An attacker with the ability to access, delete, or modify data from within the application could result in reputational damage for the business through the impact on customers' trust. This can also result in indirect financial costs to the business through fines and regulatory bodies if sensitive data is accessed. The severity of the impact on the business is dependent on the sensitivity of the data being stored in, and transmitted by the application.

Summary

Lower privileged user (Read-only Access user) is not allowed to Edit/Take action in plugin management section , Only Admin users (Users with privileges) are allowed to Edit/Take action on it but from the Direct Request, a Lower privileged user (Read-only Access user) can Edit the admin Environment by enabling/disabling/Cleanup plugins without privileges
As mentioned in the website : Read-only Access Group to gain read-only access Plugin Manager: List plugins (ONLY)

Proof of Concept

Send the following request using burp proxy using read-only user cookies

Note : you can change the command to (enable /disable/ cleanup) and this could be applied for all plugins (*That's why availability is High in CVSS)
POST /api/plugin/pluginmanager HTTP/1.1 Host: localhost:5000 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0 Accept: application/json, text/javascript, /; q=0.01 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/json; charset=UTF-8 Cache-Control: no-cache X-Requested-With: XMLHttpRequest Content-Length: 43 Origin: http://localhost:5000 Connection: close Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors Sec-Fetch-Site: same-origin Cookie: session_P5000= {{ Read-only access user cookies }}
{"plugin":"corewizard","command":"disable"}

Impact

Lower privileged user (Read-only Access user) can Edit the admin environment by enabling/disabling/Cleanup plugins without privileges

References

- Vulnerable section
- POC

CVE
CVE-2022-3068
(Published)

Vulnerability Type
CWE-269: Improper Privilege Management

Severity
Medium (5.3)

Registry
Other

Affected Version
1.8.2

Visibility
Public

Status

Fixed

Found by

ahmedelsadat198

@ahmedelsadat198

unranked

Fixed by

Gina Häußge

@foosel

maintainer

This report was seen 865 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

ahmedelsadat198 3 months ago Researcher

Hello, Any update here?

Charlie Powell 3 months ago Maintainer

Security reports will be processed next week.

We have sent a follow up to the **octoprint** team. We will try again in 7 days. 3 months ago

ahmedelsadat198 3 months ago Researcher

A gentle reminder.

A **octoprint/octoprint** maintainer has acknowledged this report 3 months ago

Gina Häußge 3 months ago

Patience is a virtue.

Gina Häußge modified the Severity from High (8.2) to Medium (5.3) 3 months ago

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

Gina Häußge validated this vulnerability 3 months ago

I can verify this issue, however I disagree with your severity scoring. I arrive at a CVSS vector string of CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

Explanation:

AV:L - you need an existing session and thus somehow need to take over the browser of an existing victim user. While OctoPrint CAN be configured to give guests read-only access, it doesn't ship like that and the functionality isn't heavily advertised either. Combined with the fact that OctoPrint is supposed to be run in a secured LAN environment only and public exposing on hostile networks like the internet is actively discouraged throughout documentation and even by OctoPrint itself, at the very most this could be AV:A which would turn this into 5.5 Medium.
PR:L - obviously HIGH was wrong here
S:U - there is absolutely no Scope Change possible here and I'd like to get an explanation from you what made you come to a different conclusion.
C:L - an attacker can gain more information about installed plugins than supposed to
I:L - an attacker can delete stale settings
A:L - an attacker can *mark* existing plugins as disabled or uninstall them. However, a reboot of the system is needed for this to actually lead to an availability loss and the attacker doesn't have the rights to that. So they have to rely on partially unloaded plugins misfunctioning for availability loss, and they cannot control which plugins are affected. At most, we could set UI:R here to factor the required restart into the calculation, but even then the attacker cannot deny access to the whole platform functionality and thus there is no total availability loss here.

Please elaborate how you arrived at AV:N, PR:H, S:C, A:H in your scoring. The CVSS spec is quite clear on how vulnerabilities should be scored (isolated, not as a chain) and especially how Impact is supposed to be scored.

ahmedelsadat198 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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

ahmedelsadat198 2 months ago Researcher

Any update about the remediation?

Gina Häußge 2 months ago Maintainer

It's in the works as part of a bigger bugfix release. Meanwhile I'm still waiting for your elaboration on your AV:N, PR:H, A:H and especially S:C scoring.

We have sent a third and final fix follow up to the **octoprint** team. This report is now considered stale. 2 months ago

Gina Häußge marked this as fixed in **1.8.3** with commit **ef95ef** 2 months ago

Gina Häußge has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us