Insufficient Session Expiration After Password Change in cockpit-hq/cockpit

0

Valid Reported on Aug 5th 2022

Description

During my test, I found that in Cockpit v 2.1.2, the application was not validating the request after password change. This allows attacker to update user account details even after admin changes password.

Steps to Reproduce :

Login with your account and click on click on "Account Settings" and update your details and intercept the request in Burpsuite/Owasp Zap.
Now change your account password and try changing your account details from from the request we just captured before changing password.
You will notice that the application returns following response.
{"error": "401", "message":"Unauthorized request"}
Now refresh the page. You will notice that our admins account details have successfully changed.

Proof Of Concept: https://drive.google.com/file/d/1yqwYB1o8jfXtPUTgQ_yzI_sRqkfAyXx3/view?usp=sharing

Impact

If admin's account gets compromised, even if admin changes his password, attacker is still able to update admin account details and perform malicious actions.

CVE
CVE-2022-2713
(Published)

Vulnerability Type

CWE-613: Insufficient Session Expiration

Severity
High (8.6)

Registry
Other

Affected Version
2.1.2 (2022-08-04)

Visibility
Public

Status
Fixed

Found by

whoisshuvam
@whoisshuvam
master

Fixed by

Artur
@aheinze
maintainer

This report was seen 695 times.

We are processing your report and will contact the **cockpit-hq/cockpit** team within 24 hours. 4 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 4 months ago

We have contacted a member of the **cockpit-hq/cockpit** team and are waiting to hear back 4 months ago

Artur validated this vulnerability 4 months ago

I can validate the issue and will provide a fix. Thanks for reporting!

whoisshuvam has been awarded the disclosure bounty ✓

whoisshuvam has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Artur marked this as fixed in 2.2.0 with commit dd8d03 4 months ago

Artur has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

whoisshuvam 4 months ago Researcher

Hi @admin ,
Can you please assign an CVE for this issue 🙂 if accepted by @maintainer .

Kind Regards,
Suvam Adhikari

❤ Artur gave praise 4 months ago

Thank you for the finding 🙏 Go for the CVE!

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Jamie Slome 4 months ago Admin

CVE assigned and should be published in the next 24 hours 👍

Well done all! 🎉

Sign in to join this conversation

Chat with us