huntr

2FA Bypass in Cockpit Content Platform ≤ v2.2.1 in cockpit-hq/cockpit

0

✓ Valid Reported on Aug 11th 2022

Description

2FA secret is disclosed in JWT token after user logs into his account in Cockpit Content Platform ≤ v2.2.1 allowing attacker to bypass the 2FA code.

Proof of Concept

1.Login with your admin account and enable 2FA in your account and logout.
2.Go to http://yourserver.com/cockpit221/auth/login and enter your username and password and intercept the request in BurpSuite or Owasp Zap.
3.Now, Click perform following action "Right click > Do intercept > Response to this request" and forward the request.
4.Now you will get a response like this from http://yourserver.com/cockpit221/auth/check.

```
HTTP/1.0 200 OK
Date: Thu, 11 Aug 2022 11:24:32 GMT
Server: Apache/2.4.53 (Unix) OpenSSL/1.1.1o PHP/8.1.6 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.1.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 520
Connection: close
Content-Type: application/json
{"success":true,"user":
{"name":"Suvam","user":"suvam","email":"admin@suvam.com","twofa":"eyJ0eXAiOiJKV1QiLCJh
bGciOiJIUzI1NiJ9.eyJ1c2VyIjoic3V2YW0iLCJlbWFpbCI6ImFkbWluQHN1dmFtLmNvbSIsImFjdGl2
ZSI6dHJ1ZSwibmFtZSI6IlN1dmFtIiwiaTE4biI6ImVuIiwicm9sZSI6ImFkbWluIiwidGhlbWUiOiJhdXR
vIiwiX21vZGlmaWVkIjoxNjYwMjE2OTczLCJfY3JlYXRlZCI6MTY2MDIxNDU5OS
FhZWI2MjM1NjVkZGM3MDAwMzRlIiwidHdvZmEiOnsiZW5hYmxlZCI6dHJ1ZSwic2VjcmV0IjoiMj
dPWUNJSVpJQ1JFR0JUVUFPVUVTQzNHM1BXNUJ2Q04ifX0.Q5DL1nZy4bYl8909luvBZso4Fnszl
```

dPWUNJ3VpJQ1JERUJUVUFPVUV1Q2NHM1BXNU02Q04ifX0.Q5DL1pZv4bY1o9U9luvRzse4FhszL FOGIVCvGVcqbDk"}}

5.Now, copy the payload of JWT token and decode it. The structure of JWT token is like this header.payload.signature .

6.Decode the payload. You will notice that the Authentication Secret token is disclosed in the payload JWT token.

7.Copy the Authenticator Secret token and provide it to Google Authenticator . @2FA is bypassed.

8.Attacker can exploit this vulnerability to bypass 2FA.

Proof Of Concept Video : https://drive.google.com/file/d/1rKCtY5W7XyIuApHtVAdWOusHJpw8b8OF/view?usp=sharing

Impact

Account Takeover

CVE
CVE-2022-2818
(Published)

Vulnerability Type
CWE-305: Authentication Bypass by Primary Weakness

Severity
Critical (9.8)

Registry
Other

Affected Version
2.2.1

Visibility
Public

Status
Fixed

Found by

whoisshuvam
@whoisshuvam
master

Chat with us

Fixed by

Artur

@aheinze

maintainer

This report was seen 688 times.

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

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

Artur 3 months ago Maintainer

Hi 👋 One question. You said that the attacker would decode the JWT payload. But how would the attacker know the secret to decode the payload?

Cheers
Artur

Artur 3 months ago Maintainer

Ahh, my bad. Yes, that needs to be fixed 👍

Artur validated this vulnerability 3 months ago

Fix is on the way

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 **2.2.2** with commit **4bee1b** 3 months ago

Chat with us

Artur has been awarded the fix bounty ✓

Artur has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✖

❤ Artur gave praise 3 months ago

Thank you very much for reporting 🙏

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

whoisshuvam 3 months ago Researcher

Hi @maintainer ,

Thanks for quick fix. May I know when will the next release be published?

Kind Regards,
@whoisshuvam

Artur 3 months ago Maintainer

v2.2.2 is planned for Monday (2022-08-15)

whoisshuvam 3 months ago Researcher

Hi @admin ,

Can you make the report private. The new release v2.2.2 will be made on Monday. Hi @maintainer , I would be glad if you could approve for CVE.

Kind Regards,
@whoisshuvam

Artur 3 months ago Maintainer

approved 👍

whoisshuvam 3 months ago

Hi @admin,

Can you please assign an CVE for this vulnerability 😇 since its approved by maintainer and fix has been deployed.

Kind Regards,
Suvam

Jamie Slome 3 months ago Admin

Sorted 👍

Sign in to join this conversation