huntr

Authentication Bypass Using an Alternate Path or Channel in requarks/wiki

4

✓ Valid   Reported on May 8th 2022

Steps to reproduce

1. Log into Administrator account
2. Navigate to User section
3. Create a new User, call it testUser pass is 12345678
4. Navigate to Groups section and create a new group, call it testGroup
5. Give a "manage:group" permission for testGroup and assign testUser to group
6. Log into testUser account and navigate to Groups --> Permissions section
7. Click on Update Group and intercept it by BurpSuit Iterceptor
8. Change "permissions":["manage:groups"], to "permissions":["manage:system"]
9. Relog in and obverse that we can manage system
10. It can't be done via GUI
11. Video PoC: https://youtu.be/yd0uFCwEBiE

Impact

User can get root user permissions

CVE
CVE-2022-1681
(Published)

Vulnerability Type
CWE-288: Authentication Bypass Using an Alternate Path or Channel

Severity
High (7.2)

Registry
Npm

Chat with us

Affected Version
2.5.280

Visibility
Public

Status
Fixed

Found by

n1k1x86
@n1k1x86
unranked

Fixed by

Nicolas Giard
@ngpixel
maintainer

This report was seen 733 times.

We are processing your report and will contact the **requarks/wiki** team within 24 hours.
7 months ago

We have contacted a member of the **requarks/wiki** team and are waiting to hear back
7 months ago

Nicolas Giard validated this vulnerability 7 months ago

n1k1x86 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Nicolas Giard marked this as fixed in **2.5.281** with commit **78d02d** 7 months ago

Nicolas Giard has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

n1k1x86 7 months ago Researcher

n1k1x86 7 months ago Researcher

Greets! Are you not against assigning a CVE as a maintainer? Huntr will do it all automatically with your agreement. Thanks for the reply in advance! This vulnerability was found in collaboration with @scara31 (https://huntr.dev/users/scara31)

n1k1x86 7 months ago Researcher

@admin Hey, sorry for the ping, could you please assign a CVE for this one if maintainer doesn't mind it?

Jamie Slome 6 months ago Admin

Sorted 👍

n1k1x86 6 months ago Researcher

Hi! I'm very pleased, thank you!

Sign in to join this conversation

contact us

terms

privacy policy

Chat with us