`defaultGroup` ID and access is retained after access to said group ("collection") is removed

High **tankerkiller125** published **GHSA-6pvm-v73p-p6m9** 4 days ago

Package

ghcr.io/sysadminsmedia.homebox (Docker)

Affected versions	Patched versions
0.24.0-0.24.2	>0.24.2

sysadminsmedia/homebox (Docker)

0.24.0-0.24.2	>0.24.2

Description

Summary

`defaultGroup` ID was permanently assigned to an invited user, even when access from said group was removed. This user was not able to modify/view contents of said group in the Web interface but could make changes via API.

Impact

User B cannot modify/view *Collection A* via Web UI.
User B CAN make CRUD actions to *Collection A* via API, despite access being revoked.
User B's properties still list the original group ID as their `defaultGroup` ID, and that `defaultGroup` was not correctly validated when the `X-Tenant` header was not set thereby permitting access.

Severity

High 8.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVE ID

CVE-2026-40196

Weaknesses

- CWE-708
- CWE-862

Credits

tmeuze	Reporter
tankerkiller125	Remediation developer