



# Remnawave Backend has a race condition in HWID device limit allows bypassing max devices

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-39880
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 20:16:26 UTC
<b>Updated</b>	2026-04-17 20:38:20 UTC
<b>Description</b>	Remnawave Backend is the backend for the Remnawave proxy and user management solution. Prior to 2.7.5, a glitch in th

## Risk And Classification

**Primary CVSS:** v3.1 4.9 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000290000 probability, percentile 0.081200000 (date 2026-04-17)

**Problem Types:** CWE-362 | CWE-362 CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:L
3.1	security-advisories@github.com	Secondary	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	DECLARED	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

Low

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Remnawave	Remnawave Backend	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Remnawave	Backend	affected < 2.7.5	Not specified

#### References

Reference	Source	Link	Tags
github.com/remnawave/backend/security/advisories/GHSA-985p-44h5-v3pq	security-advisories@github.com	github.com	Exploit, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)