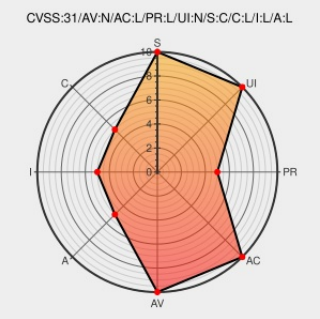
CVE-2021-43829

Published on: Not Yet Published

Last Modified on: 12/17/2021 04:28:00 PM UTC

CVE-2021-43829 - advisory for GHSA-5hc9-6hq4-2xfx

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Patrowlmanager from Patrowl contain the following vulnerability:

PatrOwl is a free and open-source solution for orchestrating Security Operations. In versions prior to 1.7.7 PatrowlManager unrestrictly handle upload files in the findings import feature. This vulnerability is capable of uploading dangerous type of file to server leading to XSS attacks and potentially other forms of code injection. Users are advised to update to 1.7.7 as soon as possible. There are no known workarounds for this issue.

CVE-2021-43829 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Patrowl** - **PatrowlManager** version **< 1.7.7**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Unrestricted Upload of File with Dangerous Type · Advisory · Patrowl/PatrowlManager · GitHub	github.com text/html	CONFIRM github.com/Patrowl/PatrowlManager/security/advisories/GHSA-5hc9-6hq4-3
Unrestricted Upload of File with Dangerous Type vulnerability found in patrowlmanager	huntr.dev text/html	MISC huntr.dev/bounties/17324785-f83a-4058-ac40-03f2bfa16399/
Fix Unrestricted Upload of File with Dangerous Type (from Huntr bug b… · Patrowl/PatrowlManager@2287c97 · GitHub	github.com text/html	MISC github.com/Patrowl/PatrowlManager/commit/2287c9715d2e7ef11b44bb0ad4a57727654f2

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Patrowl	Patrowlmanager	All	All	All	All

cpe:2.3:a:patrowl:patrowlmanager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@prophaze	CVE-2021-43829 prophaze.com/cve/cve-2021-4…	2021-12-14 23:04:03
/r/netcve	CVE-2021-43829	2021-12-14 19:38:57

← Previous ID

Next ID→