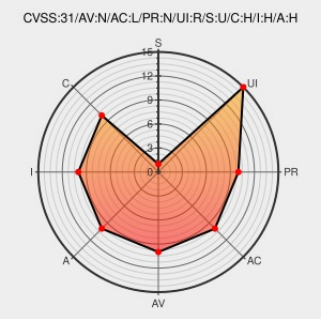
CVE-2023-23721

Published on: Not Yet Published

Last Modified on: 03/23/2023 03:09:00 PM UTC

CVE-2023-23721

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



Certain versions of Admin Log from Admin Log Project contain the following vulnerability:

Cross-Site Request Forgery (CSRF) vulnerability in David Gwyer Admin Log plugin <= 1.50 versions.

CVE-2023-23721 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **David Gwyer** - **Admin Log** version **<= 1.50**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
WordPress Admin Log plugin <= 1.50 - Cross Site Request Forgery (CSRF) vulnerability - Patchstack	patchstack.com text/html	MISC patchstack.com/database/vulnerability/admin-log/wordpress-admin-log-plugin-1-50-cross-site-request-forgery-csrf-vulnerability?_s_id=cve

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Admin Log Project	Admin Log	All	All	All	All

cpe:2.3:a:admin_log_project:admin_log:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-23721 : Cross-Site Request Forgery CSRF vulnerability in David Gwyer Admin Log plugin <= 1.50 versions..... twitter.com/i/web/status/1…	2023-03-20 12:06:09
/r/netcve	CVE-2023-23721	2023-03-20 12:38:36

← Previous ID

Next ID→