



CVE-2021-29435

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

Summary

CVE	CVE-2021-29435
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-13 20:15:00 UTC
Updated	2021-04-19 15:19:00 UTC
Description	trestle-auth is an authentication plugin for the Trestle admin framework. A vulnerability in trestle-auth versions 0.4.0 and 0.4

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trestle-auth Project	Trestle-auth	0.4.0	All	All	All
Application	Trestle-auth Project	Trestle-auth	0.4.1	All	All	All

References

Reference	Source	Lin
Ensure CSRF protection is prepended before authentication before_actions · TrestleAdmin/trestle-auth@cb95b05 · GitHub	MISC	gith
Cross-Site Request Forgery (CSRF) in trestle-auth · Advisory · TrestleAdmin/trestle-auth · GitHub	CONFIRM	gith
trestle-auth RubyGems.org your community gem host	MISC	rub
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

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

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