



CVE-2021-41583

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2021-41583
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-24 03:15:00 UTC
Updated	2024-03-12 17:33:00 UTC
Description	vpn-user-portal (aka eduVPN or Let's Connect!) before 2.3.14, as packaged for Debian 10, Debian 11, and Fedora, allows i

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Eduvpn	Vpn-user-portal	All	All	All	All
Operating System	Fedoraproject	Fedora	-	All	All	All

References

Reference	Source	Link	Tags
Releases · eduvpn/vpn-user-portal · GitHub	Scraper	github.com	Release Notes, Third Party Advisory
[eduVPN-deploy] Details Security Issue 2021-08-25	MISC	list.surfnet.nl	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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