CVE-2023-29713

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-29713
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-09 19:15:00 UTC
Updated	2023-06-16 17:57:00 UTC
Description	Cross Site Scripting vulnerability found in Vade Secure Gateway allows a remote attacker to execute arbitrary code via a cr

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vadesecure	Secure Gateway	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-29713 – Reflected XSS in Vade Secure Gateway – YLabs	MISC	labs.yarix.com	
info.vadesecure.com/hubfs/Ressource%20Marketing%20Website/Datasheet/EN/Vade_Secur...	MISC	info.vadesecure.com	
Vade | AI-Powered, Collaborative Email Security	MISC	www.vadesecure.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report