



CVE-2023-29712

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

Summary

CVE	CVE-2023-29712
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-09 18:15:00 UTC
Updated	2023-06-16 17:30:00 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	Vadeseure	Secure Gateway	All	All	All	All

References

Reference	Source	Link
info.vadeseure.com/hubfs/Ressource%20Marketing%20Website/Datasheet/EN/Vade_Secur...	MISC	info.vadeseure.com
Vade Secure Gateway Multiple XSS (CVE-2023-29712, CVE-2023-29713, CVE-2023-29714) – YLabs	MISC	labs.yarix.com
Vade AI-Powered, Collaborative Email Security	MISC	www.vadeseure.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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