



CVE-2021-4020

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

Summary

CVE	CVE-2021-4020
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-27 10:15:00 UTC
Updated	2021-11-30 19:27:00 UTC
Description	janus-gateway is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Meetecho	Janus	All	All	All	All

References

Reference	Source	Link	Tags
Cross-site Scripting (XSS) - Stored vulnerability found in janus-gateway	CONFIRM	huntr.dev	
Fix potential Cross-site Scripting (XSS) exploits in demos · meetecho/janus-gateway@d3fc00e · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[184996](#) Debian Security Update for janus (CVE-2021-4020)

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