CVE-2021-39206

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-39206
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-09 23:15:00 UTC
Updated	2021-09-27 18:30:00 UTC
Description	Pomerium is an open source identity-aware access proxy. Envoy, which Pomerium is based on, contains two authorization

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Envoyproxy	Envoy	All	All	All	All
Application	Envoyproxy	Envoy	1.19.0	All	All	All
Application	Pomerium	Pomerium	All	All	All	All
Application	Pomerium	Pomerium	0.15.0	All	All	All

References

Reference	Source	Link
Security releases of Envoy 1.19.1, 1.18.4, 1.17.4, and 1.16.5 are now available	MISC	group
Incorrectly handling of URI '#fragment' element as part of the path element · Advisory · envoyproxy/envoy · GitHub	MISC	github
Incorrect Authorization with specially crafted requests · Advisory · pomerium/pomerium · GitHub	CONFIRM	github
Incorrect concatenation of multiple value request headers in ext-authz extension · Advisory · envoyproxy/envoy · GitHub	MISC	github
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981066 Go (go) Security Update for github.com/pomerium/pomerium (GHSA-cfc2-wjcm-c8fm)

© CVE.report 2026 |
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 registred 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.

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