CVE-2018-20744

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

Summary

CVE	CVE-2018-20744
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-28 08:29:00 UTC
Updated	2019-02-20 18:59:00 UTC
Description	The Olivier Poitrey Go CORS handler through 1.3.0 actively converts a wildcard CORS policy into reflecting an arbitrary Ori

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Go Cors Project	Go Cors	All	All	All	All

References

Reference	Source	Link
www.usenix.org/system/files/conference/usenixsecurity18/sec18-chen.pdf	MISC	www.usenix
CORS security: reflecting any origin header value when configured to * is dangerous · Issue #55 · rs/cors · GitHub	MISC	github.com
Go CORS Handler CVE-2018-20744 Security Bypass Vulnerability	BID	www.securit
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.