CVE-2020-5207

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-5207
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-27 20:15:00 UTC
Updated	2020-02-04 14:41:00 UTC
Description	In Ktor before 1.3.0, request smuggling is possible when running behind a proxy that doesn't handle Content-Length and Tr

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetbrains	Ktor	All	All	All	All
Application	Jetbrains	Ktor	All	All	All	All

References

Reference	Source	Link
Request smuggling is possible when both chunked TE and content length specified · Advisory · ktorio/ktor · GitHub	CONFIRM	github.com
Fix CIO headers and chunked parsers by cy6erGn0m · Pull Request #1547 · ktorio/ktor · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983112 Java (maven) Security Update for io.ktor:ktor-server-cio (GHSA-xrr9-rh8p-433v)

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