



CVE-2020-7611

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

Summary

CVE	CVE-2020-7611
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-30 22:15:00 UTC
Updated	2020-04-02 14:37:00 UTC
Description	All versions of io.micronaut:micronaut-http-client before 1.2.11 and all versions from 1.3.0 before 1.3.2 are vulnerable to HT

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Objectcomputing	Micronaut	All	All	All	All
Application	Objectcomputing	Micronaut	All	All	All	All

References

Reference

- [Validate client headers · micronaut-projects/micronaut-core@9d1eff5 · GitHub](#)
- [CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers \('HTTP Request Header Injection'\) · Advisory · micronaut-projects/m](#)
- [HTTP Request Header Injection in io.micronaut:micronaut-http-client | Snyk](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980505](#) Java (maven) Security Update for io.micronaut:micronaut-http-client (GHSA-694p-xrhg-x3wm)

© [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 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](#)