



CVE-2020-36319

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

Summary

CVE	CVE-2020-36319
State	PUBLIC
Assigner	security@vaadin.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 16:15:00 UTC
Updated	2022-09-20 19:28:00 UTC
Description	Insecure configuration of default ObjectMapper in com.vaadin:flow-server versions 3.0.0 through 3.0.5 (Vaadin 15.0.0 throu

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vaadin	Flow	All	All	All	All
Application	Vaadin	Vaadin	All	All	All	All

References

Reference
CVE-2020-36319: Potential sensitive data exposure in applications using Vaadin 15
[Security Fix]Use Vaadin's own ObjectMapper instead of the one from Spring by haijian-vaadin · Pull Request #8016 · vaadin/flow · GitHub
inherit the default behaviour of spring for internal object mapper by haijian-vaadin · Pull Request #8051 · vaadin/flow · GitHub
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered and responsibly reported by Christian Knoop (<https://github.com/knoobie>).

Legacy QID Mappings

© [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](#)