



# CVE-2021-31406

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

## Summary

<b>CVE</b>	CVE-2021-31406
<b>State</b>	PUBLIC
<b>Assigner</b>	security@vaadin.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-23 16:15:00 UTC
<b>Updated</b>	2021-04-30 19:01:00 UTC
<b>Description</b>	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vaadin	Flow	All	All	All	All
Application	Vaadin	Flow	6.0.0	-	All	All
Application	Vaadin	Vaadin	All	All	All	All
Application	Vaadin	Vaadin	19.0.0	-	All	All

## References

Reference	Source	Link
Use time-constant comparison for CSRF tokens in endpoint by haijian-vaadin · Pull Request #10157 · vaadin/flow · GitHub	CONFIRM	<a href="#">github</a>
CVE-2021-31406: Timing side channel vulnerability in endpoint request handler in Vaadin 15-19	CONFIRM	<a href="#">vaadin</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** This issue was discovered and responsibly reported by Xhelal Likaj.

## 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](#)