



Unauthorized session creation via reserved framework path access

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

Summary

CVE	CVE-2026-2742
State	PUBLISHED
Assigner	Vaadin
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:18:49 UTC
Updated	2026-05-07 18:40:35 UTC
Description	An authentication bypass vulnerability exists in Vaadin 14.0.0 through 14.14.0, 23.0.0 through 23.6.6, 24.0.0 through 24.9.7

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from security@vaadin.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:N/AU:Y/R:A/V:D/RE:L/U:Amber

Problem Types: CWE-284 | NVD-CWE-Other | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
4.0	security@vaadin.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/E:X
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/S:N
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:N/AU:Y/R:A/V:D/RE:L/U:Amber

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	Vaadin	Vaadin	affected 10.0.0 14.14.0 maven	Not specified
CNA	Vaadin	Vaadin	affected 15.0.0 23.6.6 maven	Not specified
CNA	Vaadin	Vaadin	affected 24.0.0 24.9.7 maven	Not specified
CNA	Vaadin	Vaadin	affected 25.0.0 25.0.1 maven	Not specified
CNA	Vaadin	Flow	affected 1.0.0 2.13.0 maven	Not specified
CNA	Vaadin	Flow	affected 3.0.0 23.6.7 maven	Not specified
CNA	Vaadin	Flow	affected 24.0.0 24.9.7 maven	Not specified
CNA	Vaadin	Flow	affected 25.0.0 25.0.1 maven	Not specified

References

Reference	Source	Link	Tags
github.com/vaadin/flow/pull/23037	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/22998	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23052	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23034	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23033	security@vaadin.com	github.com	Issue Tracking, Patch
github.com/vaadin/flow/pull/23057	security@vaadin.com	github.com	Issue Tracking, Patch
vaadin.com/security/cve-2026-2742	security@vaadin.com	vaadin.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Users of affected versions should apply the following mitigation or upgrade.

There are currently no legacy QID mappings associated with this CVE.

© [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

