CVE

VEX

Public o

Last mo

Description | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | FAQ

Description

A flaw was found in Undertow. When Undertow receives an HTTP request where the first header line starts with one or more spaces, it incorrectly processes the request by stripping these leading spaces. This behavior, which violates HTTP standards, can be exploited by a remote attacker to perform request smuggling. Request smuggling allows an attacker to bypass security mechanisms, access restricted information, or manipulate web caches, potentially leading to unauthorized actions or data exposure.

Additional information

- Bugzilla 2443262: undertow: Undertow: Request Smuggling via Malformed HTTP Request Headers
- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

External references

- https://www.cve.org/CVERecord?id=CVE-2026-28369
- https://nvd.nist.gov/vuln/detail/CVE-2026-28369

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat build of Apache Camel for Spring Boot 4
Components	undertow-core
State	Affected
Justification	None
Errata	
Release Date	

Products / Services	Red Hat build of Apache Camel - HawtIO 4
Components	undertow-core
State	Affected
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Data Grid 8

1-10 of 17

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD

	Red Hat	NVD
CVSS v3 Base Score	8.7	N/A
Attack Vector	Network	N/A
Attack Complexity	High	N/A
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Changed	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	N/A
Availability Impact	None	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors? ›

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: March 27, 2026 at 4:13:08 PM UTC

⚠ Partial system outage