CVE-2026-28368

VEX

Public on August 27, 2025

Last modified: March 31, 2026 at 6:31:30 PM UTC

IMPORTANT

Important severity

What does this mean?

8.7

CVSS v3 Score Breakdown

Jump to section

Description

A flaw was found in Undertow. This vulnerability allows a remote attacker to construct specially crafted requests where header names are parsed differently by Undertow compared to upstream proxies. This discrepancy in header interpretation can be exploited to launch request smuggling attacks, potentially bypassing security controls and accessing unauthorized resources.

Statement

This flaw in Undertow's header parsing logic allows for request smuggling attacks when U ndertow is deployed behind an upstream proxy. Crafted requests can bypass security con trols by being interpreted differently by Undertow and the proxy, potentially leading to un authorized access or cache poisoning.

Mitigation

Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

Additional information

- Bugzilla 2443261: undertow: Undertow: Request smuggling via inconsistent header parsing
- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

External references

- https://www.cve.org/CVERecord?id=CVE-2026-28368
- https://nvd.nist.gov/vuln/detail/CVE-2026-28368

Affected Packages and Issued Red Hat Security Errata

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.

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	Not affected
Justification	Vulnerable Code not in Execute Path
Errata	
Release Date	

Products / Services	Red Hat Data Grid 8
Components	undertow-core
State	Will not fix
Justification	None
Errata	

1 of 2

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	CVE List
CVSS v3 Base Score	8.7	9.1	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	Low	N/A
Privileges Required	None	None	N/A
User Interaction	None	None	N/A
Scope	Changed	Unchanged	N/A
Confidentiality Impact	High	High	N/A
Integrity Impact	High	High	N/A
Availability Impact	None	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

NVD: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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 31, 2026 at 6:31:30 PM UTC

Red Hat Summit