



Bug 2443261 (CVE-2026-28368) - CVE-2026-28368 undertow: Undertow: Request smuggling via inconsistent header parsing

Keywords: Security

Reported: 2026-02-27 04:44 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-03-27 16:00 UTC ([History](#))

Alias: CVE-2026-28368

CC List: 50 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-27 04:44:48 UTC

[Description](#)

Undertow splits header names from values on either space or colon, whichever comes first. This allows for the construction of crafted requests with headers that are visible only to Undertow, but not upstream proxies, which can be used to launch request smuggling attacks.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

