



## Bug 2443262 (CVE-2026-28369) - CVE-2026-28369 undertow: Undertow: Request Smuggling via Malformed HTTP Request Headers

**Keywords:** Security

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

**Status:** NEW

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

**Alias:** CVE-2026-28369

**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 DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**

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

**Attachments** ([Terms of Use](#))

OSIDB Bzimport 2026-02-27 04:44:52 UTC

[Description](#)

When Undertow receives a request in which the first header line begins with one or more spaces, it strips them before processing the request. This is usable as a request smuggling primitive.

The HTTP RFCs state that when a field-line begins with a space or tab, it is permissible to concatenate it into the previous field-line's value. This is referred to as `obs-fold` in the RFCs. However, it is always invalid to obs-fold on the first line, since there is no

previous field-line to concatenate into. Thus, the message should be rejected.

---

Note

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

