



Undertow: undertow: request smuggling via inconsistent header parsing

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

Summary

CVE	CVE-2026-28368
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 17:16:27 UTC
Updated	2026-03-31 18:20:30 UTC
Description	A flaw was found in Undertow. This vulnerability allows a remote attacker to construct specially crafted requests where hear

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from nvd@nist.gov

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

EPSS: 0.000820000 probability, percentile 0.241260000 (date 2026-04-01)

Problem Types: CWE-444 | CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	secalert@redhat.com	Secondary	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Build Of Apache Camel - Hawtio	4.0	All	All	All
Application	Redhat	Build Of Apache Camel For Spring Boot	4.0	All	All	All
Application	Redhat	Data Grid	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Fuse	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	8.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform Expansion Pack	-	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Undertow	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Apache Camel For Spring Boot 4	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Apache Camel - HawtIO 4	Not specified	Not specified
CNA	Red Hat	Red Hat Data Grid 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat Fuse 7	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified

CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat Process Automation 7	Not specified	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
access.redhat.com/security/cve/CVE-2026-28368	secalert@redhat.com	access.redhat.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

Source	Time	Event
CNA	2026-02-27T04:39:57.578Z	Reported to Red Hat.
CNA	2025-08-27T00:00:00.000Z	Made public.

Workarounds

CNA: 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.

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](#).

CVE.report and Source URL Uptime Status status.cve.report