Undertow: undertow: request smuggling via `\r\r\r` as a header block terminator

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-28367
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 17:16:27 UTC
Updated	2026-03-30 13:26:29 UTC
Description	A flaw was found in Undertow. A remote attacker can exploit this vulnerability by sending `\r\r\r` as a header block terminatc

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from secalert@redhat.com

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

EPSS: 0.000360000 probability, percentile 0.103840000 (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	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

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

None

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

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	
access.redhat.com/security/cve/CVE-2026-28367	secalert@redhat.com	access.redhat.com	
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	2026-02-27T00:00:00.000Z	Reported to Red Hat.
CNA	2025-08-27T00:00:00.000Z	Made public.

Workarounds

CNA: To mitigate this vulnerability, configure any proxy servers positioned in front of Undertow to strictly validate HTTP header terminations. Ensure that these proxies are configured to reject or normalize non-standard header block terminators, such as `\r\r\r`, before forwarding requests to Undertow. This operational control helps prevent request smuggling attacks by ensuring that only properly formed HTTP requests reach the Undertow server.

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 registred 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