Undertow: outofmemory when parsing form data encoding with application/x-www-form-urlencoded

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2024-3884
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-03 19:15:54 UTC
Updated	2026-03-30 12:16:18 UTC
Description	A flaw was found in Undertow that can cause remote denial of service attacks. When the server uses the FormEncodedDat

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.009410000 probability, percentile 0.761840000 (date 2026-04-01)

Problem Types: CWE-20 | CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.1 EUS For RHEL 7	unaffected 0:1.4.18-19.SP17_redhat_00001.1.ep
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.1 EUS For RHEL 7	unaffected 0:7.1.14-4.GA_redhat_00003.1.ep7.el
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.3 EUS For RHEL 7	unaffected 0:2.0.41-7.SP8_redhat_00001.1.el7ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.3 EUS For RHEL 7	unaffected 0:7.3.17-5.GA_redhat_00006.1.el7eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 7	unaffected 0:2.2.39-1.Final_redhat_00001.1.el7ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 7	unaffected 0:7.4.24-4.GA_redhat_00002.1.el7eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 8	unaffected 0:2.2.39-1.Final_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 8	unaffected 0:7.4.24-4.GA_redhat_00002.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 9	unaffected 0:2.2.39-1.Final_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 9	unaffected 0:7.4.24-4.GA_redhat_00002.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:1.83.0-1.redhat_00001.1.el8eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:33.0.0-2.jre_redhat_00003.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:4.0.6-1.redhat_00001.1.el8eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:1.0.0-3.redhat_00009.1.el8eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:2.0.2-1.Final_redhat_00001.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 8	unaffected 0:2.3.23-1.SP3_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:1.83.0-1.redhat_00001.1.el9eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:33.0.0-2.jre_redhat_00003.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:4.0.6-1.redhat_00001.1.el9eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:1.0.0-3.redhat_00009.1.el9eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:2.0.2-1.Final_redhat_00001.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.0 For RHEL 9	unaffected 0:2.3.23-1.SP3_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:4.0.10-1.redhat_00001.1.el8eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:1.82.0-1.redhat_00001.1.el8eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:801.3.0-1.GA_redhat_00001.1.el8ea

CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:1.0.1-3.redhat_00003.1.el8eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:6.6.36-1.Final_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:4.0.2-1.Final_redhat_00001.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:2.5.0-1.redhat_00001.1.el8eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:2.3.20-2.SP4_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:8.1.3-4.GA_redhat_00006.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:5.0.12-1.Final_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:2.6.6-1.Final_redhat_00001.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 8	unaffected 0:8.1.1-4.GA_redhat_00007.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:4.0.10-1.redhat_00001.1.el9eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:1.82.0-1.redhat_00001.1.el9eap * rp
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:801.3.0-1.GA_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:1.0.1-3.redhat_00003.1.el9eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:6.6.36-1.Final_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:4.0.2-1.Final_redhat_00001.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:2.5.0-1.redhat_00001.1.el9eap * rpm
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:2.3.20-2.SP4_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:8.1.3-4.GA_redhat_00006.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:5.0.12-1.Final_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:2.6.6-1.Final_redhat_00001.1.el9eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8.1 For RHEL 9	unaffected 0:8.1.1-4.GA_redhat_00007.1.el9eap
CNA	Red Hat	OpenShift Serverless	Not specified
CNA	Red Hat	Red Hat Build Of Apache Camel 4 For Quarkus 3	Not specified
CNA	Red Hat	Red Hat Build Of Apache Camel For Spring Boot 3	Not specified
CNA	Red Hat	Red Hat Build Of Apache Camel For Spring Boot 4	Not specified
CNA	Red Hat	Red Hat Build Of Apache Camel - HawtIO 4	Not specified
CNA	Red Hat	Red Hat Build Of Apicurio Registry 2	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified
CNA	Red Hat	Red Hat Build Of OptaPlanner 8	Not specified
CNA	Red Hat	Red Hat Build Of Quarkus	Not specified
CNA	Red Hat	Red Hat Build Of Quarkus	Not specified
CNA	Red Hat	Red Hat Data Grid 8	Not specified
CNA	Red Hat	Red Hat Fuse 7	Not specified
CNA	Red Hat	Red Hat Integration Camel K 1	Not specified
CNA	Red Hat	Red Hat Integration Camel Quarkus 2	Not specified

CNA	Red Hat	Red Hat JBoss Data Grid 7	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified
CNA	Red Hat	Red Hat JBoss Fuse Service Works 6	Not specified
CNA	Red Hat	Red Hat Process Automation 7	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified
CNA	Red Hat	Streams For Apache Kafka	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:6011	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2024-3884	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3889	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4924	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0386	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6012	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4916	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3891	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3892	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0383	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4915	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0384	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4917	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	2024-04-16T00:00:00.000Z	Reported to Red Hat.
CNA	2025-12-03T16:50:50.000Z	Made public.

Workarounds

CNA: It is possible to mitigate the vulnerability by performing an upper-level verification to ensure the content size sent server side is within the allowed parameters.

There are currently no legacy QID mappings associated with this CVE.

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