CVE-2024-3884

VEX

Public on December 3, 2025
Last modified: December 4, 2025 at 3:57:10 PM UTC

MODERATE

Moderate severity
What does this mean?

7.5

CVSS v3 Score Breakdown

Jump to section

Description | Statement | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | FAQ

Description

A flaw was found in Undertow that can cause remote denial of service attacks. When the server uses the FormEncodedDataDefinition.doParse(StreamSourceChannel) method to parse large form data encoding with application/x-www-form-urlencoded, the method will cause an OutOfMemory issue. This flaw allows unauthorized users to cause a remote denial of service (DoS) attack.

Statement

Red Hat rates this as a Moderate impact since this requires the use of a specific form method by the server that must be externally available and the input is not sanitized by the given servlet or class implementing its use.

Mitigation

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.

Additional information

- Bugzilla 2275287: undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded
- CWE-20: Improper Input Validation

External references

- https://www.cve.org/CVERecord?id=CVE-2024-3884
- https://nvd.nist.gov/vuln/detail/CVE-2024-3884

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	Red Hat JBoss Enterprise Application Platform 7.1 EUS for RHEL 7

Components	eap7-undertow
State	Fixed
Justification	None
Errata	RHSA-2026:6012
Release Date	March 30, 2026

Products / Services	Red Hat JBoss Enterprise Application Platform 7.1 EUS for RHEL 7
Components	eap7-wildfly
State	Fixed
Justification	None
Errata	RHSA-2026:6012
Release Date	March 30, 2026

1-10 of 46

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	7.5	N/A
Attack Vector	Network	N/A
Attack Complexity	Low	N/A
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	None	N/A
Integrity Impact	None	N/A
Availability Impact	High	N/A

CVSS v3 Vector

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

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors? ›

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: December 4, 2025 at 3:57:10 PM UTC

⚠ Partial system outage