CVE-2026-3260

VEX

Public on March 24, 2026

Last modified: April 8, 2026 at 7:34:15 PM UTC

MODERATE

Moderate severity

What does this mean?

5.9

CVSS v3 Score Breakdown

Jump to section

Description

A flaw was found in Undertow. A remote attacker could exploit this vulnerability by sending an HTTP GET request containing multipart/form-data content. If the underlying application processes parameters using methods like `getParameterMap()`, the server prematurely parses and stores this content to disk. This could lead to resource exhaustion, potentially resulting in a Denial of Service (DoS).

Statement

This vulnerability in Undertow, as utilized in Wildfly, allows for premature parsing and stor age of multipart/form-data content to disk when an HTTP GET request is received. Expl oitation occurs only if the underlying application, such as JSF, explicitly invokes parameter-parsing methods like getParameterMap(). Red Hat products are affected when running applications that meet these specific conditions.

Mitigation

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.

Additional information

- Bugzilla 2443010: undertow: Undertow: Denial of Service due to premature multipart/form-data parsing in GET requests
- CWE-770: Allocation of Resources Without Limits or Throttling

External references

- https://www.cve.org/CVERecord?id=CVE-2026-3260
- https://nvd.nist.gov/vuln/detail/CVE-2026-3260

Affected Packages and Issued Red Hat Security Errata

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.

Search:

Filter by: Products / Services | Components | State

Errata Clear all

Products / Services	Red Hat build of Apache Camel for Spring Boot 4
Components	undertow-core
State	Fix deferred
Justification	None
Errata	
Release Date	

Products / Services	Red Hat build of Apache Camel - HawtIO 4
Components	undertow-core
State	Fix deferred
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Data Grid 8
Components	undertow-core
State	Fix deferred
Justification	None
Errata	

1 of 2

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).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	5.9	7.5	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	Low	N/A
Privileges Required	None	None	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	None	None	N/A
Availability Impact	High	High	N/A

CVSS v3 Vector

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

NVD: 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?**

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: April 8, 2026 at 7:34:15 PM UTC

Red Hat Summit