



# Libsoup: null pointer dereference in libsoup may lead to denial of service

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

## Summary

<b>CVE</b>	CVE-2025-4476
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-05-16 18:16:10 UTC
<b>Updated</b>	2026-05-06 16:16:03 UTC

**Description** A denial-of-service vulnerability has been identified in the libsoup HTTP client library. This flaw can be triggered when a libs

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from secalert@redhat.com

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

**Problem Types:** CWE-476 | CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	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

#### References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
gitlab.gnome.org/GNOME/libsoup/-/issues/440	secalert@redhat.com	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	
access.redhat.com/security/cve/CVE-2025-4476	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
gitlab.gnome.org/GNOME/libsoup/-/work_items/440	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

#### Additional Advisory Data

Source	Time	Event
CNA	2025-05-15T14:21:35.587Z	Reported to Red Hat.
CNA	2025-05-08T00:00:00.000Z	Made public.

#### Workarounds

**CNA:** To mitigate the risk posed by this libsoup vulnerability, Red Hat strongly advises against connecting client applications relying on the libsoup library to untrusted HTTP servers until systems can be updated to a version of libsoup that includes the fix for this specific flaw. This precaution will help prevent potential denial-of-service scenarios within user sessions.

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)