



# Libsoup: heap buffer overflow in sniff\_unknown()

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

## Summary

<b>CVE</b>	CVE-2025-32052
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-04-03 14:15:44 UTC
<b>Updated</b>	2026-04-22 11:16:01 UTC
<b>Description</b>	A flaw was found in libsoup. A vulnerability in the sniff_unknown() function may lead to heap buffer over-read.

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from secalert@redhat.com

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

**EPSS:** 0.011150000 probability, percentile 0.782340000 (date 2026-04-22)

**Problem Types:** CWE-126 | CWE-126 Buffer Over-read

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.62.3-8.el8_10 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.8-3.el8_10.1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:8.10-1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.62.3-8.el8_10 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Extended Update Support	unaffected 0:2.62.3-3.el8_8.4 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.72.0-10.el9_6.1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Extended Update Support	unaffected 0:2.72.0-8.el9_2.4 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.72.0-8.el9_4.4 * rpm	Not specified
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

### References

Reference	Source	Link	Tags
lists.debian.org/debian-its-announce/2025/04/msg00036.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>	
access.redhat.com/security/cve/CVE-2025-32052	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:8292	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:4508	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:4440	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
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/425	secalert@redhat.com	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	
access.redhat.com/errata/RHSA-2025:7436	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:4560	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:4568	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</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,

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Additional Advisory Data

Source	Time	Event
CNA	2025-04-03T01:16:47.177Z	Reported to Red Hat.
CNA	2025-04-03T00:00:00.000Z	Made public.

#### Workarounds

**CNA:** No mitigation is currently available for this vulnerability.

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](#)