



Libsoup: oob read on libsoup through function "soup_multipart_new_from_message" in soup-multipart.c leads to crash or exit of process

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

Summary

CVE	CVE-2025-32914
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-14 15:15:25 UTC
Updated	2026-04-22 11:16:02 UTC
Description	A flaw was found in libsoup, where the soup_multipart_new_from_message() function is vulnerable to an out-of-bounds read

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from secalert@redhat.com

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

EPSS: 0.005210000 probability, percentile 0.669220000 (date 2026-04-22)

Problem Types: CWE-125 | CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.6.5-3.el10_0 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:2.62.2-9.el7_9 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:2.62.2-6.el7_9 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.62.3-9.el8_10 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.62.3-9.el8_10 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:2.62.3-1.el8_2.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:2.62.3-2.el8_4.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:2.62.3-2.el8_6.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:2.62.3-2.el8_6.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:2.62.3-2.el8_6.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Extended Update Support	unaffected 0:2.62.3-3.el8_8.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.72.0-10.el9_6.2 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.72.0-8.el9_0.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Extended Update Support	unaffected 0:2.72.0-8.el9_2.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.72.0-8.el9_4.5 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified

References

Reference	Source	Link	Tags
lists.debian.org/debian-lts-announce/2025/04/msg00036.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2025:9179	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8252	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8481	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8140	secalert@redhat.com	access.redhat.com	
gitlab.gnome.org/GNOME/libsoup/-/issues/436	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/errata/RHSA-2025:8126	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8482	secalert@redhat.com	access.redhat.com	

access.redhat.com/errata/RHSA-2025:8663	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:21657	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-32914	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:7505	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8132	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8480	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8139	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-04-14T01:21:01.384Z	Reported to Red Hat.
CNA	2025-04-14T00:00:00.000Z	Made public.

Workarounds

CNA: Currently, no mitigation is 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](#)