Libsoup: heap buffer overflow in sniff_unknown()

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-32052
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-03 14:15:44 UTC
Updated	2026-04-22 11:16:01 UTC
Description	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-lts-announce/2025/04/msg00036.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/security/cve/CVE-2025-32052	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8292	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4508	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4440	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
gitlab.gnome.org/GNOME/libsoup/-/issues/425	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/errata/RHSA-2025:7436	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4560	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4568	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

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.