Libsoup: libsoup: information disclosure via cleartext transmission of cookies during https tunnel establishment

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-5119
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 07:15:58 UTC
Updated	2026-04-01 17:45:57 UTC
Description	A flaw was found in libsoup. When establishing HTTPS tunnels through a configured HTTP proxy, sensitive session cookies

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from nvd@nist.gov

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

EPSS: 0.000200000 probability, percentile 0.051970000 (date 2026-04-01)

Problem Types: CWE-319 | CWE-319 Cleartext Transmission of Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
3.1	secalert@redhat.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Libsoup	-	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

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
gitlab.gnome.org/GNOME/libsoup/-/issues/502	secalert@redhat.com	gitlab.gnome.org	Exploit, Issue Tracking
access.redhat.com/security/cve/CVE-2026-5119	secalert@redhat.com	access.redhat.com	Vendor Advisory, Mitigation
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Kona Arctic for reporting this issue. (en)

Additional Advisory Data

Additional Advisory Data

Source	Time	Event
CNA	2026-03-30T05:15:27.541Z	Reported to Red Hat.
CNA	2026-03-30T05:30:32.610Z	Made public.

Workarounds

CNA: To mitigate this issue, ensure that all HTTP proxies used for HTTPS tunnels are trusted and operate within a secure network. Avoid configuring applications to use untrusted HTTP proxies. If feasible, configure applications to bypass proxies for sensitive connections or utilize a secure proxy solution that encrypts the entire communication channel. A service restart or application reload may be required for changes to take effect.

There are currently no legacy QID mappings associated with this CVE.