



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

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

## Summary

<b>CVE</b>	CVE-2026-5119
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-30 07:15:58 UTC
<b>Updated</b>	2026-04-01 17:45:57 UTC
<b>Description</b>	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
<a href="https://gitlab.gnome.org/GNOME/libsoup/-/issues/502">gitlab.gnome.org/GNOME/libsoup/-/issues/502</a>	secalert@redhat.com	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>	Exploit, Issue Tracking
<a href="https://access.redhat.com/security/cve/CVE-2026-5119">access.redhat.com/security/cve/CVE-2026-5119</a>	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	Vendor Advisory, Mitigation
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking, Vendor Advisory
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

### 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.

© [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](#).

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