Bug 2452932 (CVE-2026-5119) - CVE-2026-5119 libsoup: libsoup: Information disclosure via cleartext transmission of cookies during HTTPS tunnel establishment

Keywords: Security

Status: NEW

Alias: CVE-2026-5119

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2452934 2452935 2452936

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-30 05:15 UTC by OSIDB Bzimport

Modified: 2026-03-30 05:34 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-30 05:15:51 UTC Description

```
Cleartext Transmission of Sensitive Information has been
reported in libsoup’s HTTP CONNECT handling. When establishing
HTTPS tunnels via soup_session.c::tunnel_connect(), cookies
(including potentially sensitive session cookies) are sent in
cleartext within the initial HTTP CONNECT request to the
configured proxy. A network-positioned attacker or malicious
HTTP proxy can intercept or observe these cookies and leverage
them for session hijacking or user impersonation.
```

Note

You need to log in before you can comment on or make changes to this bug.