



Bug 2442909 (CVE-2026-2436) - CVE-2026-2436 libsoup: libsoup: Denial of Service via use-after-free in SoupServer during TLS handshake

Keywords: Security ✕

Reported: 2026-02-26 01:15 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-03-10 15:51 UTC ([History](#))

Alias: CVE-2026-2436

CC List: 0 users

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Version: unspecified

Environment:

Hardware: All

Last Closed:

OS: Linux

Embargoed:

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-26 01:15:07 UTC

[Description](#)

SoupServer is vulnerable to use after free vulnerability because `soup_server_disconnect()` frees all `SoupServerConnection` objects, even if there is a pending GNUTLS handshake to be finished.

A TLS handshake is initiated asynchronously. After creating the `SoupServerConnection`, `libsoup` calls `g_tls_connection_handshake_async()`, which registers `tls_connection_handshake_ready_cb` as a callback. The handshake runs in the background and the callback fires later when it completes.

When the TLS handshake completes successfully, GNUTLS invokes `tls_connection_handshake_ready_cb()` asynchronously

soup_server_disconnect() is called (due to some scenario, like a server restart, or other cases). This iterates through all active connections and disconnects them. When the last reference to a SoupServerConnection is dropped, soup_server_connection_finalize() is called, freeing the object.

If the TLS handshake

completes after soup_server_disconnect() has freed the connection object, tls_connection_handshake_ready_cb() still fires with a dangling pointer. The callback then calls soup_server_connection_connected(conn), which attempts to access the freed SoupServerConnection via soup_server_connection_get_iostream(), causing a crash

Note

You need to [log in](#) before you can comment on or make changes to this bug.

