



Bug 2445762 (CVE-2026-3832) - CVE-2026-3832 gnutls: gnutls: Security bypass allows acceptance of revoked server certificates via crafted OCSP response

Keywords:

Reported: 2026-03-09 13:57 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-05-03 18:47 UTC ([History](#))

Alias: CVE-2026-3832

CC List: 8 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: low

Severity: low

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 2026-03-09 13:57:29 UTC

[Description](#)

gnutls matches a stapled ocsp response to the server certificate by scanning SingleResponse records, but then reads cert_status from record index 0 unconditionally. when a multi-record ocsp response is stapled such that record 0 is for a different certificate (good) and the matching record for the server certificate is later (revoked), a client with ocsp verification enabled can accept a revoked server certificate. this is observable as an order-dependent accept/reject outcome for the same revoked server certificate.

Note

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

