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

Keywords: Security

Status: NEW

Alias: CVE-2026-3832

Product: Security Response

Component: vulnerability

Version: unspecified

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

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

Modified: 2026-05-04 08:40 UTC (History)

CC List: 10 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Flags: mcascell: needinfo?

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.