Bug 2445763 (CVE-2026-3833) - CVE-2026-3833 gnutls: GnuTLS: Policy bypass due to case-sensitive nameConstraints comparison

Keywords: Security

Status: NEW

Alias: CVE-2026-3833

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-09 14:03 UTC by OSIDB Bzimport

Modified: 2026-05-03 18:49 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-09 14:03:06 UTC Description

```
gnutls compares nameConstraints labels using a case-sensitive
memcmp path without an ascii-casefold canonicalization step.
when excludedSubtrees/permittedSubtrees dNSName (dns) or
rfc822Name (email) constraints are present, attacker-
controlled casing differences in the leaf certificate SAN can
cause a false accept (policy bypass) where the certificate
should be rejected.
```

Note

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