GnuTLS backend silently skips certificate chain verification when verify_peer is false

High **sauwming** published **GHSA-x2fv-6j6c-pxmx** 2 weeks ago

Package

No package listed

Affected versions

2.16 or earlier

Patched versions

2.17

Description

On GnuTLS builds, the SIP TLS transport (`sip_transport_tls`) can accept connections with invalid or untrusted certificates even when the application explicitly enables certificate verification via `verify_server = PJ_TRUE` or `verify_client = PJ_TRUE`.

Impact

Only GnuTLS builds are affected (`--with-gnutls`). OpenSSL and Apple SecureTransport/Network.framework builds are **not** affected.

- Client mode (verify_server = PJ_TRUE): a network-positioned attacker can present an untrusted, expired, or self-signed certificate and complete a TLS handshake, enabling man-in-the-middle of outbound SIPS connections.
- Server mode (verify_client = PJ_TRUE): the server accepts any client certificate, bypassing mutual-TLS authentication.

Patches

The patch is available as commit `ef68425` in the master branch.

Workarounds

App can temporarily switch to the other SSL backends.

References

If you have any questions or comments about this advisory:
Email us at security@pjsip.org

Severity

High

CVE ID

CVE-2026-42225

Weaknesses

No CWEs

Credits

feynman-hou Reporter