

# [gnutls-help] gnutls 3.8.10

Daiki Ueno [ueno@gnu.org](mailto:ueno@gnu.org)

Wed Jul 9 07:01:58 CEST 2025

- Previous message (by thread): [\[gnutls-help\].guile-gnutls copy at codeberg](#)
  - Next message (by thread): [\[gnutls-help\].guile-gnutls-5.0.0 released \[stable\]](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)
- 

Hello,

We have just released gnutls-3.8.10. This is a bug fix, security and enhancement release on the 3.8.x branch.

We would like to thank everyone who contributed in this release: Alexander Sosedkin, Andrew Hamilton, Angel Yankov, Daiki Ueno, Daniel P. Berrangé, David Dudas, Doekin, František Krenželok, Jiasheng Jiang, Richard Hughes, and Zoltan Fridrich.

The detailed list of changes follows:

- \* Version 3.8.10 (released 2025-07-08)
- \*\* libgnutls: Fix NULL pointer dereference when 2nd Client Hello omits PSK  
Reported by Stefan Bühler. [GNUTLS-SA-2025-07-07-4, CVSS: medium] [CVE-2025-6395]
- \*\* libgnutls: Fix heap read buffer overrun in parsing X.509 SCTS timestamps  
Spotted by oss-fuzz and reported by OpenAI Security Research Team, and fix developed by Andrew Hamilton. [GNUTLS-SA-2025-07-07-1, CVSS: medium] [CVE-2025-32989]
- \*\* libgnutls: Fix double-free upon error when exporting otherName in SAN  
Reported by OpenAI Security Research Team. [GNUTLS-SA-2025-07-07-2, CVSS: low] [CVE-2025-32988]
- \*\* certtool: Fix 1-byte write buffer overrun when parsing template  
Reported by David Aitel. [GNUTLS-SA-2025-07-07-3, CVSS: low] [CVE-2025-32990]
- \*\* libgnutls: PKCS#11 modules can now be used to override the default cryptographic backend. Use the [provider] section in the system-wide config to specify path and pin to the module (see system-wide config Documentation).
- \*\* libgnutls: Linux kernel version 6.14 brings a Kernel TLS (kTLS) key update support. The library running on the aforementioned version now utilizes the kernel's key update mechanism when kTLS is enabled, allowing uninterrupted TLS session. The --enable-ktls configure option as well as the system-wide kTLS configuration(see GnuTLS Documentation) are still required to enable this feature.
- \*\* libgnutls: liboqs support for PQC has been removed  
For maintenance purposes, support for post-quantum cryptography (PQC) is now only provided through leancrypto. The experimental key exchange algorithm, X25519Kyber768Draft00, which is based on the round 3 candidate of Kyber and only supported through liboqs has also been removed altogether.
- \*\* libgnutls: TLS certificate compression methods can now be set with cert-compression-alg configuration option in the gnutls priority file.

\*\* libgnutls: All variants of ML-DSA private key formats are supported  
While the previous implementation of ML-DSA was based on draft-ietf-lamps-dilithium-certificates-04, this updates it to draft-ietf-lamps-dilithium-certificates-12 with support for all 3 variants of private key formats: "seed", "expandedKey", and "both".

\*\* libgnutls: ML-DSA signatures can now be used in TLS  
The ML-DSA signature algorithms, ML-DSA-44, ML-DSA-65, and ML-DSA-87, can now be used to digitally sign TLS handshake messages.

\*\* API and ABI modifications:

GNUTLS\_PKCS\_MLDSA\_SEED: New enum member of gnutls\_pkcs\_encrypt\_flags\_t

GNUTLS\_PKCS\_MLDSA\_EXPANDED: New enum member of gnutls\_pkcs\_encrypt\_flags\_t

## Getting the Software

=====

GnuTLS may be downloaded directly from

<https://www.gnupg.org/ftp/gcrypt/>

A list of GnuTLS mirrors can be found at

<http://www.gnutls.org/download.html>

Here are the XZ compressed sources:

<https://www.gnupg.org/ftp/gcrypt/gnutls/v3.8/gnutls-3.8.10.tar.xz>

Here are OpenPGP detached signatures signed using key:

462225C3B46F34879FC8496CD605848ED7E69871

<https://www.gnupg.org/ftp/gcrypt/gnutls/v3.8/gnutls-3.8.10.tar.xz.sig>

Note that it has been signed with my openpgp key:

pub rsa4096 2009-07-23 [SC] [expires: 2026-06-29]

462225C3B46F34879FC8496CD605848ED7E69871

uid [ultimate] Daiki Ueno <[ueno\\_at\\_unixuser.org](mailto:ueno_at_unixuser.org)>

uid [ultimate] Daiki Ueno <[ueno\\_at\\_gnu.org](mailto:ueno_at_gnu.org)>

sub rsa4096 2010-02-04 [E]

Regards,

--

Daiki Ueno

----- next part -----

A non-text attachment was scrubbed...

Name: signature.asc

Type: application/pgp-signature

Size: 832 bytes

Desc: not available

URL: <<https://lists.gnupg.org/pipermail/gnutls-help/attachments/20250709/3576eeff/attachment.sig>>

- 
- Previous message (by thread): [\[gnutls-help\].guile-gnutls copy at codeberg](#)
  - Next message (by thread): [\[gnutls-help\].guile-gnutls-5.0.0 released \[stable\]](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)

---

[More information about the Gnutls-help mailing list](#)