- **About Security Advisories**

  Although, the core GnuTLS team does not have resources to analyse the background and impact of security issues in depth, we do take security seriously. All known information on high or critical security vulnerabilities is collected and published in this page..

- **Reporting security problems**

  Report non-public reports to the issue tracker as confidential, or send an email to the bug report mail address.

Advisories

Tag	Other identifiers	Description	Information
GNUTLS-SA-2026-04-29-9	CVE-2026-42014	Severity Medium; use-after-free	Changing the Security Officer PIN with gnutls_pkcs11_token_set_pin() with oldpin == NULL for a token lacking a protected authentication path led to a use-after-free. The issue was reported in the issue tracker as #1766 by Luigino Camastra and Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-8	CVE-2026-42013	Severity Medium; certificate misuse	Validation of certificates with oversized Subject Alternative Names would fall back to checking DNS hostnames against Common Name. The issue was independently reported in the issue tracker as #1825 and #1849 by Haruto Kimura (Stella) and Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-7	CVE-2026-42012	Severity Medium; certificate misuse	Certificates containing URI or SRV Subject Alternative Names would fall back to checking DNS hostnames against Common Name, allowing potential misuse of such certificates beyond their original purpose. The issue was reported in the issue tracker as #1802 by Oleh Konko (1seal). **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-6	CVE-2026-42011	Severity Medium; name constraint bypass	Permitted name constraints were wrongfully ignored when prior CAs only had excluded name constraints, resulting in a name constraint bypass. The issue was reported in the issue tracker as #1824 by Haruto Kimura (Stella). **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-5	CVE-2026-3833	Severity Moderate; name constraint bypass	Domain name comparison during name constraints processing was case-sensitive, violating RFC 5280 section 7.2. For excluded name constraints, this could lead to incorrectly accepting domain names that should've been rejected. The issue was originally reported in the issue tracker as #1223, and then independently re-reported as a security issue by #1803 and #1852 by Oleh Konko (1seal) and Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.

GNUTLS-SA-2026-04-29-4	CVE-2026-42010	Severity High; authentication bypass	Servers configured with RSA-PSK wrongfully matched usernames with NUL character in them to ones truncated to NUL character, which could lead to an authentication bypass. The issue was reported in the issue tracker as #1850 by Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-3	CVE-2026-33845	Severity High; heap overrun	A remotely triggerable underflow in the DTLS reassembly code led to a heap overrun. The issue was reported in the issue tracker as #1811 by Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-2	CVE-2026-42009	Severity High; undefined behaviour	The comparator function used for ordering DTLS packets by sequence numbers did not follow qsort comparator contracts in case of packets with duplicate sequence numbers, which could lead to undefined behaviour. The issue was reported in the issue tracker as #1848 by Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-13	CVE-2026-5419	Severity Low; timing side-channel	The PKCS#7 padding check performed during decryption was not constant-time, potentially leaking information about the padding bytes through timing differences. The issue was reported in the issue tracker as #1815 by Doria Tang of Stony Brook University. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-12	CVE-2026-3832	Severity Low; revocation bypass	When validating a certificate against a multi-entry OCSP response, the revocation status was always checked for the first entry instead of the entry matching the certificate, which could lead to accepting revoked certificates. The issue was independently reported in the issue tracker as #1801 and #1812 by Oleh Konko (1seal) and Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-11	CVE-2026-42015	Severity Low; out-of-bounds write	Appending to a PKCS#12 bag that already contained 32 elements could write past the bag's internal array. The issue was reported in the issue tracker as #1840 by Zou Dikai. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-10	CVE-2026-5260	Severity Medium; heap overread	For a server using an RSA key backed by a PKCS#11 token, a client sending an extremely short premaster secret during an RSA key exchange could trigger a short heap overread. The issue was reported in the issue tracker as #1814 by Joshua Rogers of AISLE Research Team. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-04-29-1	CVE-2026-33846	Severity High; heap overwrite	GnuTLS didn't check that DTLS fragments claimed a consistent message_length value. Additionally, a crucial array size check was missing, enabling an attacker to cause a heap overwrite. The issue was independently reported in the issue tracker as #1816, #1838 and #1839 by Haruto Kimura (Stella), Oscar Reparaz and Zou Dikai.

			Recommendation: To address the issue found, upgrade to GnuTLS 3.8.13 or later versions.
GNUTLS-SA-2026-02-09-2	CVE-2025-14831	Severity Medium; denial of service	Verifying certificates with pathological amounts of name constraints could lead to a denial of service attack via resource exhaustion. The issue was reported in the issue tracker as #1773 by Tim Scheckenbach. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.12 or later versions.
GNUTLS-SA-2026-02-09-1	CVE-2026-1584	Severity High; invalid pointer access	A TLS 1.3 resumption attempt with an invalid PSK binder value in ClientHello could lead to a denial of service attack via crashing the server. The issue was reported in the issue tracker as #1790 by Jaehun Lee. **Recommendation:** To address the issue found, upgrade to GnuTLS 3.8.12 or later versions. 3.8.10 or earlier versions are not affected.
GNUTLS-SA-2025-11-18	CVE-2025-9820	Severity Low; Stack write buffer overflow	When a PKCS#11 token is initialized with gnutls_pkcs11_token_init function and it is passed a token label longer than 32 characters, it may write past the boundary of stack allocated memory. The issue was reported in the issue tracker as #1732. **Recommendation:** Given the length limit is imposed by the PKCS#11 standard, the application should check and reject longer label exceeding the limit, though this was unclear in the GnuTLS documentation. If it is not feasible for some reason, we would recommend upgrading GnuTLS to 3.8.11 or later versions. The issue could also be effectively mitigated if you compile the library with -D_FORTIFY_SOURCE=2.
GNUTLS-SA-2025-07-08-4	CVE-2025-6395	Severity Medium; Denial of service	When a TLS 1.3 handshake involves a Hello Retry Request and the second Client Hello omits the PSK which was present in the first Client Hello, the GnuTLS server can dereference a NULL pointer. The issue was reported in the issue tracker as #1718. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.10 or later versions.
GNUTLS-SA-2025-07-08-3	CVE-2025-32990	Severity Low; Heap write buffer overflow	When the certtool program is invoked with a template file with a number of string pairs for a single keyword, a NULL pointer could be written past the memory boundary. The issue was reported in the issue tracker as #1696. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.10 or later versions.
GNUTLS-SA-2025-07-08-2	CVE-2025-32988	Severity Low; Memory corruption on error path	When any error occurs during exporting a certificate with an otherName in the SAN (subject alternative name) extension, the library could potentially double free the ASN.1 structure. The issue was reported in the issue tracker as #1694. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.10 or later versions.
GNUTLS-SA-2025-07-08-1	CVE-2025-32989	Severity Medium; Heap read buffer overflow	When an X.509 certificate contains an SCT (signed certificate timestamp) extension and its length field is malformed, the library could read the memory buffer past the boundary. The issue was reported in the issue tracker as #1695. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.10 or later versions. The issue could be effectively avoided if you compile the library with -D_FORTIFY_SOURCE=2.

GNUTLS-SA-2025-02-07	CVE-2024-12243	Severity Medium; Denial of service	When a certificate contains a number of Name Constraints extensions, GnuTLS applications can take excessive amount of time to validate it against the Subject Alternative Names. The issue was reported in the issue tracker as #1553. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.9 or later versions. Also make sure to build with libtasn1 4.20.0 or later.
GNUTLS-SA-2024-01-23	CVE-2024-28835	Severity Medium; Denial of service	When validating a certificate chain with more then 16 certificates GnuTLS applications crash with an assertion failure. The issue was reported in the issue tracker as #1527 and #1525. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.4 or later versions.
GNUTLS-SA-2024-01-14	CVE-2024-0553	Severity Medium; more timing sidechannel in RSA-PSK key exchange	The previous fix for CVE-2023-5981 turned to be incomplete as it still leaves an observable difference in the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange and the one of ciphertexts with correct PKCS#1 v1.5 padding. Only TLS ciphertext processing is affected. The issue was reported in the issue tracker as #1522. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.3 or later versions.
GNUTLS-SA-2024-01-09	CVE-2024-0567	Severity Medium; Denial of service	When validating a certificate chain which contains a cycle of cross-signed signatures of multiple CA certificates, GnuTLS applications crash with an assertion failure. This affects GnuTLS 3.7.0 to 3.8.2. The issue was reported in the issue tracker as #1521. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.3 or later versions.
GNUTLS-SA-2023-12-04	CVE-2024-28834	Severity Medium; timing sidechannel in deterministic ECDSA	A vulnerability was found that the deterministic ECDSA code leaks bit-length of random nonce which allows for full recovery of the private key used after observing a few hundreds to a few thousands of signatures on known messages, due to the application of lattice techniques. The issue was reported in the issue tracker as #1516. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.4 or later versions.
GNUTLS-SA-2023-10-23	CVE-2023-5981	Severity Medium; timing sidechannel in RSA-PSK key exchange	A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. Only TLS ciphertext processing is affected. The issue was reported in the issue tracker as #1511. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.2 or later versions.
GNUTLS-SA-2022-07-07	CVE-2022-2509	Severity Medium; memory corruption	When gnutls_pkcs7_verify cannot verify signature against given trust list, it starts creating a chain of certificates starting from identified signer up to known root. During the creation of this chain the signer certificate gets freed which results in double free when the same signer certificate is freed at the end of the algorithm. This affects GnuTLS 3.6.0 to 3.7.6. The issue was reported in the issue tracker as #1383. **Recommendation:** To address the issue found upgrade to GnuTLS 3.7.7 or later versions.

GNUTLS-SA-2022-01-17	N/A	Severity Low; memory corruption	When a single trust list object is shared among multiple threads, calls to gnutls_x509_trust_list_verify_crt2() was able to corrupt temporary memory where internal copy of an issuer certificate is stored. The code path is only taken when a PKCS#11 based trust store is enabled and the issuer certificate is already stored as trusted. This affects GnuTLS 3.7.0 to 3.7.2. The issue was reported in the issue tracker as #1277. **Recommendation:** To address the issue found upgrade to GnuTLS 3.7.3 or later versions.
GNUTLS-SA-2021-03-10	CVE-2021-20231, CVE-2021-20232	Severity Low; use-after-free	It was found that the client sending a "key_share" or "pre_share_key" extension may result in dereferencing a pointer no longer valid after realloc(). This only happens in TLS 1.3 and only when the client sends a large Client Hello message, e.g., when HRR is sent in a resumed session previously negotiated large FFDHE parameters, because the initial allocation of the buffer is large enough without having to call realloc(). The issue was reported in the issue tracker as #1151. **Recommendation:** To address the issue found upgrade to GnuTLS 3.7.1 or later versions.
GNUTLS-SA-2020-09-04	CVE-2020-24659	Severity Moderate; null-pointer dereference	It was found by oss-fuzz that the server sending a "no_renegotiation" alert in an unexpected timing, followed by an invalid second handshake can cause a TLS 1.3 client to crash via a null-pointer dereference. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure. The issue was reported in the issue tracker as #1071. **Recommendation:** To address the issue found upgrade to GnuTLS 3.6.15 or later versions.
GNUTLS-SA-2020-07-14	CVE-2023-0361	Severity Medium; timing sidechannel in RSA decryption	A vulnerability was found that the response times to malformed RSA ciphertexts in ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. Only TLS ciphertext processing is affected. The issue was reported in the issue tracker as #1050. **Recommendation:** To address the issue found upgrade to GnuTLS 3.8.0 or later versions.
GNUTLS-SA-2020-06-03	CVE-2020-13777	Severity High; flaw in TLS session ticket key construction	▪ It was found that GnuTLS 3.6.4 introduced a regression in the TLS protocol implementation. This caused the TLS server to not securely construct a session ticket encryption key considering the application supplied secret, allowing a MitM attacker to bypass authentication in TLS 1.3 and recover previous conversations in TLS 1.2. See #1011 for more discussion on the topic. **Recommendation:** To address the issue found upgrade to GnuTLS 3.6.14 or later versions.
GNUTLS-SA-2020-03-31	CVE-2020-11501	Severity High; flaw in DTLS protocol implementation	▪ It was found that GnuTLS 3.6.3 introduced a regression in the DTLS protocol implementation. This caused the DTLS client to not contribute any randomness to the DTLS negotiation breaking the security guarantees of the DTLS protocol. See #960 for more discussion on the topic.

			Recommendation: To address the issue found upgrade to GnuTLS 3.6.13 or later versions.
GNUTLS-SA-2019-03-27	CVE-2019-3836 CVE-2019-3829	Severity High; invalid pointer access, double free	▪ It was found using the TLS fuzzer tools that decoding a malformed TLS1.3 asynchronous message can cause a server crash via an invalid pointer access. The issue affects GnuTLS server applications since 3.6.4. The issue was reported in issue tracker as #704. ▪ Tavis Ormandy from Google Project Zero found a memory corruption (double free) vulnerability in the certificate verification API. Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later is affected. The issue was reported in issue tracker as #694. **Recommendation:** To address the issues found upgrade to GnuTLS 3.6.7 or later versions.
GNUTLS-SA-2017-06-16	CVE-2017-7507	Severity High; null pointer dereference	It was found using the TLS fuzzer tools that decoding a status response TLS extension with valid contents could lead to a crash due to a null pointer dereference. The issue affects GnuTLS server applications. The issue was fixed in 3.5.13. **Recommendation:** To address the issues found upgrade to GnuTLS 3.5.13 or later versions.
GNUTLS-SA-2017-03-25	CVE-2017-5335 CVE-2017-5336 CVE-2017-5337	Severity High; memory corruption	It was found using the OSS-FUZZ fuzzer infrastructure that decoding a specially crafted OpenPGP certificate could lead to heap and stack overflows. This affects **only few applications which enable the OpenPGP certificate functionality** of GnuTLS. This issue was fixed in GnuTLS 3.3.26 and 3.5.8. **Recommendation:** The support of OpenPGP certificates in GnuTLS is considered obsolete. As such, it is not recommended to use OpenPGP certificates with GnuTLS. To address the issues found upgrade to GnuTLS 3.3.26, 3.5.8 or later versions.
GNUTLS-SA-2017-03-24	CVE-2017-5334	Severity High; memory corruption	It was found using the OSS-FUZZ fuzzer infrastructure that decoding a specially crafted X.509 certificate with Proxy Certificate Information extension present could lead to a double free. This issue was fixed in GnuTLS 3.3.26 and 3.5.8. **Recommendation:** Upgrade to GnuTLS 3.3.26, 3.5.8 or later versions.
GNUTLS-SA-2015-02-09	CVE-2015-3308	Severity High; memory corruption	Robert Święcki reported that decoding a specially crafted certificate with certain CRL distribution points format can lead to a double free. This issue was fixed in GnuTLS 3.3.14. **Recommendation:** Upgrade to GnuTLS 3.3.14, or later versions.
GNUTLS-SA-2014-06-03	CVE-2014-0092	Severity High; certificate verification issue	A vulnerability was discovered that affects the certificate verification functions of all gnutls versions. A specially crafted certificate could bypass certificate validation checks. The vulnerability was discovered during an audit of GnuTLS for Red Hat.

Who is affected by this attack?

- Anyone using certificate authentication in any version of GnuTLS.

How are past sessions affected?

- The vulnerability to be exploited it requires an active man-in-the-middle attacker. Past sessions are not affected unless they were under such an attack.

How to mitigate the attack?

- Upgrade to the latest GnuTLS version (3.2.12 or 3.1.22), or apply the patch for GnuTLS 2.12.x.

GNUTLS-SA-2009-08-12	CVE-2009-2730	Severity High; false positive in certificate hostname validation	Announcement of v2.8.3 that solves the problem. Analysis of the vulnerability and minimal patch. How to check if your GnuTLS library is vulnerable. Back-ported patches for earlier releases: [1] [2] **Recommendation:** Upgrade to GnuTLS 2.8.3 or later.
GNUTLS-SA-2008-08-08	CVE-2008-2377	Severity High; Denial of service on client side	Announcement Detailed analysis and patch Another report that suggest it can be exploited by hostile servers **Recommendation:** Upgrade to GnuTLS 2.4.1 or apply the patch.
GNUTLS-SA-2008-05-21	CERT-FI announcement CVE-2008-1948, CVE-2008-1949, CVE-2008-1950	Severity High; Memory corruption	Announcement and Patch Updated announcement and Patch **Recommendation:** Upgrade to GnuTLS 2.2.5 or apply the patch in the second link.
GNUTLS-SA-2006-02-06	CVE-2006-0645	Severity High; Memory corruption	Libtasn1 Announcement **Recommendation:** Upgrade to Libtasn1 0.2.18 and GnuTLS 1.2.10 (stable) or 1.3.4 (experimental).