- **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-2022-07-07	N/A	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It was found that the client sending a "key_share" or "pre_share_key" extension may result in dereferencing a pointer no longer valid after realloc().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-2020-06-03	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).