



CVE-2021-20232

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2021-20232 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-03-12 19:15:00 UTC |
| Updated | 2023-11-07 03:29:00 UTC |
| Description | A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory co |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Application | Gnu | Gnutls | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |

References

| Reference | Source |
|------------------------------------------------------------------------------------------------------------------------------|--------|
| [spark-issues] 20210430 [jira] [Commented] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| [spark-issues] 20210429 [jira] [Commented] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| Pony Mail! | MLIST |
| Pony Mail! | MLIST |
| [spark-issues] 20210413 [jira] [Created] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| GnuTLS | MISC |
| [SECURITY] Fedora 34 Update: gnutls-3.7.1-2.fc34 - package-announce - Fedora Mailing-Lists | |
| [spark-issues] 20210423 [jira] [Resolved] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| Pony Mail! | MLIST |
| [SECURITY] Fedora 34 Update: gnutls-3.7.1-2.fc34 - package-announce - Fedora Mailing-Lists | FEDORA |
| Pony Mail! | MLIST |

| | |
|------------------------------------------------------------------------------------------------------------------------------|---------|
| Pony Mail! | MLIST |
| [spark-issues] 20210426 [jira] [Updated] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| Pony Mail! | MLIST |
| [spark-issues] 20210426 [jira] [Commented] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| [spark-issues] 20210417 [jira] [Commented] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| Pony Mail! | MLIST |
| March 2021 GnuTLS Vulnerabilities in NetApp Products NetApp Product Security | CONFIR |
| Pony Mail! | MLIST |
| [spark-issues] 20210425 [jira] [Commented] (SPARK-35054) Getting Critical Vulnerability CVE-2021-20231 on spark 3.0.0 branch | |
| 1922275 – (CVE-2021-20232) CVE-2021-20232 gnutls: Use after free in client_send_params in lib/ext/pre_shared_key.c | MISC |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159515](#) Oracle Enterprise Linux Security Update for gnutls and nettle (ELSA-2021-4451)
- [159717](#) Oracle Enterprise Linux Security Update for gnutls (ELSA-2022-9221)
- [174833](#) SUSE Enterprise Linux Security update for gnutls (SUSE-SU-2021:0934-1)
- [174836](#) SUSE Enterprise Linux Security update for gnutls (SUSE-SU-2021:0935-1)
- [174852](#) SUSE Enterprise Linux Security update for gnutls (SUSE-SU-2021:0934-1)
- [174855](#) SUSE Enterprise Linux Security update for gnutls (SUSE-SU-2021:0935-1)
- [180169](#) Debian Security Update for gnutls28 (CVE-2021-20232)
- [198448](#) Ubuntu Security Notification for GnuTransport Layer Security vulnerabilities (USN-5029-1)
- [239785](#) Red Hat Update for gnutls and nettle security (RHSA-2021:4451)
- [281477](#) Fedora Security Update for gnutls (FEDORA-2021-18bef34f05)
- [296059](#) Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)
- [296060](#) Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021)
- [500235](#) Alpine Linux Security Update for gnutls
- [501415](#) Alpine Linux Security Update for gnutls
- [503982](#) Alpine Linux Security Update for gnutls
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005. ICSA-22-104-13)

| |
|------------------------------------------------------------------------------------|
| 670487 EulerOS Security Update for gnutls (EulerOS-SA-2021-2245) |
| 670513 EulerOS Security Update for gnutls (EulerOS-SA-2021-2271) |
| 671037 EulerOS Security Update for gnutls (EulerOS-SA-2021-2632) |
| 750298 OpenSUSE Security Update for gnutls (openSUSE-SU-2021:0470-1) |
| 900025 CBL-Mariner Linux Security Update for gnutls 3.6.14 |
| 901035 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (6447-1) |
| 903112 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (3973) |
| 940170 AlmaLinux Security Update for gnutls and nettle (ALSA-2021:4451) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)