



# CVE-2021-33560

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2021-33560   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-06-08 11:15:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:35:00 UTC  |
| <b>Description</b>     | Libcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address |

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product  | Version | Update |
|------------------|-------------------------------|--|---------|--------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a>   | 9.0     | All    |
| Operating System | <a href="#">FedoraProject</a> | <a href="#">Fedora</a>   | 33      | All    |
| Operating System | <a href="#">FedoraProject</a> | <a href="#">Fedora</a>   | 34      | All    |
| Application      | <a href="#">Gnupg</a>         | <a href="#">Libcrypt</a>   | All     | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Binding Support Function</a>                  | 1.11.0  | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Function Cloud Native Environment</a> | 1.10.0  | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Function Cloud Native Environment</a> | 1.9.0   | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Repository Function</a>               | 1.14.0  | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Repository Function</a>               | 1.15.0  | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Repository Function</a>               | 1.15.1  | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Network Slice Selection Function</a>          | 1.8.0   | All    |
| Application      | <a href="#">Oracle</a>        | <a href="#">Communications Cloud Native Core Service Communication Proxy</a>               | 1.15.0  | All    |

## References

| Reference  | Source | Link                                    | Tag |
|--|--------|---|-----|
| libcrypt: Multiple Vulnerabilities (GLSA 202210-13) — Gentoo security                        | GENTOO | <a href="#">security.gentoo.org</a>     |     |
| [SECURITY] Fedora 34 Update: libcrypt-1.9.3-3.fc34 - package-announce - Fedora Mailing-Lists |        | <a href="#">lists.fedoraproject.org</a> |     |

|   |         |  |     |
|---|---------|--|-----|
| Oracle Critical Patch Update Advisory - April 2022  | MISC    | <a href="http://www.oracle.com">www.oracle.com</a>                   |     |
| Oracle Critical Patch Update Advisory - October 2021  | MISC    | <a href="http://www.oracle.com">www.oracle.com</a>                   |     |
| Oracle Critical Patch Update Advisory - January 2022  | MISC    | <a href="http://www.oracle.com">www.oracle.com</a>                   |     |
| 🔗 T5466 Release Libgcrypt 1.8.8   | MISC    | <a href="http://dev.gnupg.org">dev.gnupg.org</a>                     |     |
| [SECURITY] [DLA 2691-1] libgcrypt20 security update   | MLIST   | <a href="http://lists.debian.org">lists.debian.org</a>               |     |
| [SECURITY] Fedora 33 Update: libgcrypt-1.8.8-1.fc33 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| 🔗 T5305 Release Libgcrypt 1.9.3   | MISC    | <a href="http://dev.gnupg.org">dev.gnupg.org</a>                     |     |
| [SECURITY] Fedora 33 Update: libgcrypt-1.8.8-1.fc33 - package-announce - Fedora Mailing-Lists |         | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| rCe8b7f10be275  | MISC    | <a href="http://dev.gnupg.org">dev.gnupg.org</a>                     |     |
| Oracle Critical Patch Update Advisory - July 2022   | N/A     | <a href="http://www.oracle.com">www.oracle.com</a>                   |     |
| [SECURITY] Fedora 34 Update: libgcrypt-1.9.3-3.fc34 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| 🔗 T5328 On the (in)security of Elgamal in OpenPGP   | MISC    | <a href="http://dev.gnupg.org">dev.gnupg.org</a>                     |     |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                         | can |
| NVD vulnerability detail  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       | can |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

|  |
|--|
| <a href="#">159510</a> Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2021-4409)                |
| <a href="#">159742</a> Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2022-9263)                |
| <a href="#">178682</a> Debian Security Update for libgcrypt20 (DLA 2691-1)                                   |
| <a href="#">183602</a> Debian Security Update for libgcrypt20 (CVE-2021-33560)                               |
| <a href="#">198503</a> Ubuntu Security Notification for Libgcrypt Vulnerabilities (USN-5080-1)               |
| <a href="#">239828</a> Red Hat Update for libgcrypt (RHSA-2021:4409)   |
| <a href="#">281670</a> Fedora Security Update for libgcrypt (FEDORA-2021-24d4e06195)                         |
| <a href="#">281672</a> Fedora Security Update for libgcrypt (FEDORA-2021-31fdc84207)                         |
| <a href="#">296059</a> Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021) |
| <a href="#">296060</a> Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021) |
| <a href="#">353205</a> Amazon Linux Security Advisory for libgcrypt : ALAS-2022-1578                         |
| <a href="#">353209</a> Amazon Linux Security Advisory for libgcrypt : ALAS2-2022-1769                        |
| <a href="#">354634</a> Amazon Linux Security Advisory for libgcrypt : AL2012-2022-366                        |
| <a href="#">500295</a> Alpine Linux Security Update for libgcrypt  |

|  |
|--|
| 501746 Alpine Linux Security Update for libgcrypt  |
| 504061 Alpine Linux Security Update for libgcrypt  |
| 591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13) |
| 670637 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2395)  |
| 670711 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2469)  |
| 670745 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2503)  |
| 670774 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2532)  |
| 670798 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2556)  |
| 670963 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2590)  |
| 671182 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2935)  |
| 671236 EulerOS Security Update for libgcrypt (EulerOS-SA-2022-1173)  |
| 710653 Gentoo Linux libgcrypt Multiple Vulnerabilities (GLSA 202210-13)                                      |
| 750708 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2155-1)                             |
| 750709 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2157-1)                             |
| 750711 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2156-1)                             |
| 750728 OpenSUSE Security Update for libgcrypt (openSUSE-SU-2021:0919-1)                                      |
| 750778 OpenSUSE Security Update for libgcrypt (openSUSE-SU-2021:2157-1)                                      |
| 900144 CBL-Mariner Linux Security Update for libgcrypt 1.8.7   |
| 903176 Common Base Linux Mariner (CBL-Mariner) Security Update for libgcrypt (4347)                          |
| 940222 AlmaLinux Security Update for libgcrypt (ALSA-2021:4409)  |
| 960079 Rocky Linux Security Update for libgcrypt (RLSA-2021:4409)  |

© [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](#)**