# CVE-2021-3345

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-3345 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-01-29 15:15:00 UTC |
| **Updated** | 2023-11-07 03:37:00 UTC |
| **Description** | _gcry_md_block_write in cipher/hash-common.c in Libgcrypt version 1.9.0 has a heap-based buffer overflow when the dige |

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Gnupg | Libgcrypt | 1.9.0 | All | All | All |
| Application | Gnupg | Libgcrypt | 1.9.0 | All | All | All |
| Application | Oracle | Communications Billing And Revenue Management | 12.0.0.3.0 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| git.gnupg.org Git - libgcrypt.git/commit | MISC | git.gnupg.org | Mailing |
| GnuPG (The GNU Privacy Guard) | MISC | gnupg.org | Vendor |
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www.oracle.com | |
| 767814 – (CVE-2021-3345) <dev-libs/libgcrypt-1.9.1: Exploitable buffer overflow (CVE-2021-3345) | MISC | bugs.gentoo.org | Issue Tr |
| git.gnupg.org Git - libgcrypt.git/commit | | git.gnupg.org | |
| [Announce] [Security fix] Libgcrypt 1.9.1 relased | MISC | lists.gnupg.org | Mailing |
| [Announce] [urgent] Stop using Libgcrypt 1.9.0 ! | MISC | lists.gnupg.org | Mailing |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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 registred 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**