



# CVE-2021-0308

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-0308                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | security@android.com                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2021-01-11 22:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2022-02-09 17:02:00 UTC                                                                                                    |
| <b>Description</b>     | In ReadLogicalParts of basicmbr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead |

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 11.0    | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 8.1     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 11.0    | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 8.1     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a>      | 9.0     | All    | All     | All      |

## References

| Reference                                                            | Source  | Link                                                          | Tags            |
|----------------------------------------------------------------------|---------|---------------------------------------------------------------|-----------------|
| Android Security Bulletin—January 2021   Android Open Source Project | CONFIRM | <a href="https://source.android.com">source.android.com</a>   | Vendor Advisory |
| GPT fdisk: Integer underflow (GLSA 202105-03) — Gentoo security      | GENTOO  | <a href="https://security.gentoo.org">security.gentoo.org</a> |                 |

|                                               |         |                                                         |                                  |
|-----------------------------------------------|---------|---------------------------------------------------------|----------------------------------|
| [SECURITY] [DLA 2549-1] gdisk security update | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a> | Mailing List, Third Party Advice |
| CVE Program record                            | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>           | canonical                        |
| NVD vulnerability detail                      | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>         | canonical, analysis              |

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[160234](#) Oracle Enterprise Linux Security Update for gdisk (ELSA-2022-7700)

[180116](#) Debian Security Update for gdisk (CVE-2021-0308)

[240826](#) Red Hat Update for gdisk (RHSA-2022:7700)

[500363](#) Alpine Linux Security Update for gptfdisk

[501416](#) Alpine Linux Security Update for gptfdisk

[503984](#) Alpine Linux Security Update for gptfdisk

[671577](#) EulerOS Security Update for gdisk (EulerOS-SA-2022-1532)

[671658](#) EulerOS Security Update for gdisk (EulerOS-SA-2022-1720)

[710112](#) Gentoo Linux GPT fdisk Integer underflow vulnerability (GLSA 202105-03)

[940743](#) AlmaLinux Security Update for gdisk (ALSA-2022:7700)

[960393](#) Rocky Linux Security Update for gdisk (RLSA-2022:7700)

© [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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)