



# CVE-2021-3981

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-3981   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-03-10 17:43:00 UTC   |
| <b>Updated</b>         | 2024-01-16 01:15:00 UTC   |
| <b>Description</b>     | A flaw in grub2 was found where its configuration file, known as grub.cfg, is being created with the wrong permission set all |

## Risk And Classification

**Problem Types:** CWE-276

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 34      | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Grub2</a>  | All     | All    | All     | All      |

## References

| Reference  | Source |
|--|--------|
| [SECURITY] Fedora 34 Update: grub2-2.06-9.fc34 - package-announce - Fedora Mailing-Lists   | FEDOF  |
| [SECURITY] Fedora 34 Update: grub2-2.06-9.fc34 - package-announce - Fedora Mailing-Lists   | MISC   |
| 2024170 – (CVE-2021-3981) CVE-2021-3981 grub2: Incorrect permission in grub.cfg allow unprivileged user to read the file content | MISC   |
| GRUB: Multiple Vulnerabilities (GLSA 202209-12) — Gentoo security  | GENTOO |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| oss-security - CVE-2023-4001: a password bypass vulnerability in the downstream GRUB boot manager                                |        |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| CVE Program record   | CVE.O  |
| NVD vulnerability detail   | NVD    |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|   |
|---|
| 159801 Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-2110)         |
| 184114 Debian Security Update for grub2 (CVE-2021-3981)                           |
| 240320 Red Hat Update for grub2 security (RHSA-2022:2110)                         |
| 282111 Fedora Security Update for grub2 (FEDORA-2021-8dbf0a81c0)                  |
| 282196 Fedora Security Update for grub2 (FEDORA-2021-73d63662b0)                  |
| 353265 Amazon Linux Security Advisory for grub2 : ALAS2-2022-1787                 |
| 354332 Amazon Linux Security Advisory for grub2 : ALAS2022-2022-109               |
| 354408 Amazon Linux Security Advisory for grub2 : ALAS2022-2022-043               |
| 354535 Amazon Linux Security Advisory for grub2 : ALAS-2022-109                   |
| 355137 Amazon Linux Security Advisory for grub2 : ALAS2023-2023-020               |
| 671769 EulerOS Security Update for grub2 (EulerOS-SA-2022-1819)                   |
| 671775 EulerOS Security Update for grub2 (EulerOS-SA-2022-1828)                   |
| 671912 EulerOS Security Update for grub2 (EulerOS-SA-2022-1967)                   |
| 671939 EulerOS Security Update for grub2 (EulerOS-SA-2022-1997)                   |
| 672032 EulerOS Security Update for grub2 (EulerOS-SA-2022-2268)                   |
| 672481 EulerOS Security Update for grub2 (EulerOS-SA-2023-1011)                   |
| 672521 EulerOS Security Update for grub2 (EulerOS-SA-2023-1036)                   |
| 710619 Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202209-12)                |
| 900742 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (8934)   |
| 901235 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (8937)   |
| 901359 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (8934-1) |
| 902625 Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (8937-1) |
| 940519 AlmaLinux Security Update for grub2 (ALSA-2022:2110)                       |
| 960128 Rocky Linux Security Update for grub2 (RLSA-2022:2110)                     |

© 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](#)