



# CVE-2020-14309

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

## Summary

<b>CVE</b>	CVE-2020-14309
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-30 13:15:00 UTC
<b>Updated</b>	2022-04-28 18:58:00 UTC
<b>Description</b>	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with r

## Risk And Classification

**Problem Types:** [CWE-787](#) | [CWE-190](#)

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

Reference
<a href="#">July 2020 Grub2 Vulnerabilities in NetApp Products   NetApp Product Security</a>
<a href="#">[security-announce] openSUSE-SU-2020:1168-1: important: Security update</a>
<a href="#">[security-announce] openSUSE-SU-2020:1169-1: important: Security update</a>
<a href="#">GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security</a>
<a href="#">USN-4432-1: GRUB 2 vulnerabilities   Ubuntu security notices   Ubuntu</a>
<a href="#">1852022 – (CVE-2020-14309) CVE-2020-14309 grub2: Integer overflow in grub_squash_read_symlink may lead to heap-based buffer overflo</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377345](#) Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2022:0064)

[377367](#) Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2021:0026)

[377533](#) Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2020:0108)

[502730](#) Alpine Linux Security Update for grub

[710015](#) Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)

[900056](#) CBL-Mariner Linux Security Update for grub2 2.06~rc1

[901013](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6457-1)

[903689](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1823)

[906208](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1823-1)

[906381](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6457-2)

© [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](#)