



# CVE-2020-14311

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

## Summary

<b>CVE</b>	CVE-2020-14311
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-31 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbol

## Risk And Classification

**Problem Types:** CWE-190 | CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
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
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All

## References

Reference	Source
oss-security - Re: Containers-optimized OS (COS) membership in the linux-distros list	MLIST
oss-security - Re: Containers-optimized OS (COS) membership in the linux-distros list	MLIST
1852014 – (CVE-2020-14311) CVE-2020-14311 grub2: Integer overflow in grub_ext2_read_link leads to heap-based buffer overflow	CONF
[security-announce] openSUSE-SU-2020:1168-1: important: Security update	SUSE
[security-announce] openSUSE-SU-2020:1169-1: important: Security update	SUSE
GRUB: Multiple vulnerabilities (GLSA 202104-05) — Gentoo security	GENT
USN-4432-1: GRUB 2 vulnerabilities   Ubuntu security notices   Ubuntu	UBUN
oss-security - Containers-optimized OS (COS) membership in the linux-distros list	MLIST
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">377345</a> Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2022:0064)
<a href="#">377367</a> Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2021:0026)
<a href="#">377533</a> Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2020:0108)
<a href="#">502730</a> Alpine Linux Security Update for grub
<a href="#">710015</a> Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)
<a href="#">900056</a> CBL-Mariner Linux Security Update for grub2 2.06~rc1
<a href="#">901677</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6459-1)
<a href="#">903552</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2557)
<a href="#">905793</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2557-1)
<a href="#">906281</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6459-2)

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](#)**