



# CVE-2020-10713

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-10713
<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>	2022-11-16 04:06:00 UTC
<b>Description</b>	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB veri

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Gnu	Grub2	All	All	All	All
Application	Gnu	Grub2	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Vmware	Photon Os	All	All	All	All

## References

Reference	Source
oss-security - multiple secure boot grub2 and linux kernel vulnerabilities	MLIS
VMware Knowledge Base	MISC
1825243 – (CVE-2020-10713) CVE-2020-10713 grub2: Crafted grub.cfg file can lead to arbitrary code execution during boot process	MISC
Ingress Default Backend - 404 Not Found	MISC
GRUB2 Arbitrary Code Execution Vulnerability	CISCO
July 2020 Grub2 Vulnerabilities in NetApp Products   NetApp Product Security	CONF
There's a Hole in the Boot - Eclipsium	MISC
Debian -- Security Information -- DSA-4735-1 grub2	DEBI

[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
VU#174059 - GRUB2 bootloader is vulnerable to buffer overflow	CERT
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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)
- [377414](#) Alibaba Cloud Linux Security Update for fwupd (ALINUX3-SA-2021:0048)
- [377533](#) Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2020:0108)
- [43816](#) HPE Aruba OS Multiple Security Vulnerabilities (ARUBA-PSA-2020-012)
- [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
- [900874](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6455-1)
- [902991](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1826)
- [906083](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1826-1)
- [906482](#) Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6455-2)

© 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](#)