



# CVE-2020-12888

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

## Summary

<b>CVE</b>	CVE-2020-12888
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-15 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:15:00 UTC
<b>Description</b>	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.

## Risk And Classification

**Problem Types:** CWE-755

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A700s Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Bootstrap Os</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Element Software</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	All	All	All

Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H610c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H610c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H610s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H610s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H615c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H615c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Steelstore Cloud Integrated Storage</a>	-	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	Source	Link
[SECURITY] Fedora 31 Update: kernel-5.6.15-200.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.f</a>
[SECURITY] [DLA 2420-2] linux regression update	MLIST	<a href="#">lists.d</a>
[SECURITY] Fedora 31 Update: kernel-5.6.15-200.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
USN-4526-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.u</a>
[PATCH v2 0/3] vfio-pci: Block user access to disabled device MMIO - Alex Williamson	MISC	<a href="#">lore.k</a>

[PATCH v2 3/3] vfio-pci: Invalidate mmap and block MMIO access on disabled memory - Alex Williamson	MISC	<a href="#">lore.k</a>
May 2020 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">secur</a>
[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST	<a href="#">lists.d</a>
USN-4525-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.u</a>
[PATCH v2 3/3] vfio-pci: Invalidate mmap and block MMIO access on disabled memory - Alex Williamson		<a href="#">lore.k</a>
[PATCH v2 0/3] vfio-pci: Block user access to disabled device MMIO - Alex Williamson		<a href="#">lore.k</a>
[security-announce] openSUSE-SU-2020:0935-1: important: Security update	SUSE	<a href="#">lists.o</a>
oss-security - CVE-2020-12888 Kernel: vfio: access to disabled MMIO space of some devices may lead to DoS scenario	MLIST	<a href="#">www.</a>
[SECURITY] Fedora 32 Update: kernel-5.6.14-300.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>
[security-announce] openSUSE-SU-2020:1153-1: important: Security update	SUSE	<a href="#">lists.o</a>
[SECURITY] [DLA 2420-1] linux security update	MLIST	<a href="#">lists.d</a>
[SECURITY] Fedora 32 Update: kernel-5.6.14-300.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [174728](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2020:2122-1)
- [174729](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2020:2106-1)
- [353100](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
- [353101](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
- [353102](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
- [353135](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-016
- [6140068](#) AWS Bottlerocket Security Update for kernel (GHSA-c6j2-9754-jf2x)
- [750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903619](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1930)
- [905943](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1930-1)

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](#)**