



CVE-2020-15780

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

Summary

CVE	CVE-2020-15780
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-15 22:15:00 UTC
Updated	2022-04-27 15:44:00 UTC
Description	An issue was discovered in drivers/acpi/acpi_configs.c in the Linux kernel before 5.7.7. Injection of malicious ACPI tables v

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link
oss-security - multiple secure boot grub2 and linux kernel vulnerabilities	MLIST	www.c
USN-4426-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ub
oss-security - Re: UEFI SecureBoot bypass fixes rolled out to kernels below radar	MLIST	www.c
USN-4440-1: linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ub
oss-security - UEFI SecureBoot bypass fixes rolled out to kernels below radar	MLIST	www.c
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.ker
oss-security - Re: Re: lockdown bypass on mainline kernel for loading unsigned modules	MLIST	www.c

USN-4439-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ub
american-unsigned-language-2.sh - american-unsigned-language - Disable kernel lockdown using ACPI SSDT injection	MISC	git.zx2
[security-announce] openSUSE-SU-2020:1236-1: important: Security update	SUSE	lists.op
[security-announce] openSUSE-SU-2020:1153-1: important: Security update	SUSE	lists.op
oss-security - lockdown bypass on mainline kernel for loading unsigned modules	MISC	www.c
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.7.7	MISC	cdn.ke
USN-4425-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ub
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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)
750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
900076 CBL-Mariner Linux Security Update for kernel 5.4.91
903268 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3504)
906079 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3504-1)

© [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](#)