



CVE-2021-3679

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

Summary

CVE	CVE-2021-3679
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 20:15:00 UTC
Updated	2022-10-27 12:29:00 UTC
Description	A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way us

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.14	-	All	All
Operating System	Linux	Linux Kernel	5.14	rc1	All	All
Operating System	Linux	Linux Kernel	5.14	rc2	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link	Tags
1989165 – (CVE-2021-3679) CVE-2021-3679 kernel: DoS in rb_per_cpu_empty()	MISC	bugzilla.redhat.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-4978-1 linux	DEBIAN	www.debian.org	
[SECURITY] [DLA 2843-1] linux security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159402 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9458)
159404 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9460)
159424 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9485)
159427 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9488)
159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
178809 Debian Security Update for linux (DSA 4978-1)
178844 Debian Security Update for linux-4.19 (DLA 2785-1)
178943 Debian Security Update for linux (DLA 2843-1)
179600 Debian Security Update for linux (CVE-2021-3679)
198514 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)
198515 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1)
198518 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5094-2)
198520 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)
198521 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5091-2)
198523 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2)
198524 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5096-1)
198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1)
239816 Red Hat Update for kernel security (RHSA-2021:4356)
239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
353097 Amazon Linux Security Advisory for kernel : ALAC2012-2021-033
353098 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-034
353099 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-035
353145 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-006
353156 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-004
390248 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)

671134	EulerOS Security Update for kernel (EulerOS-SA-2021-2688)
671135	EulerOS Security Update for kernel (EulerOS-SA-2021-2636)
671137	EulerOS Security Update for kernel (EulerOS-SA-2021-2713)
671181	EulerOS Security Update for kernel (EulerOS-SA-2021-2934)
671703	EulerOS Security Update for kernel (EulerOS-SA-2022-1735)
750949	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1142-1)
751155	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3192-1)
751160	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)
751163	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3206-1)
751170	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)
751437	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)
751441	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)
751451	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
751473	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
751476	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)
900294	CBL-Mariner Linux Security Update for kernel 5.10.52.1
900304	CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319	CBL-Mariner Linux Security Update for kernel 5.10.60.1
901142	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6577-1)
903451	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5121)
906190	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5121-1)
940265	AlmaLinux Security Update for kernel (ALSA-2021:4356)

© 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