



CVE-2023-1077

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

Summary

CVE	CVE-2023-1077
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-27 21:15:00 UTC
Updated	2024-01-12 17:43:00 UTC
Description	In the Linux kernel, pick_next_rt_entity() may return a type confused entry, not detected by the BUG_ON condition, as the c

Risk And Classification

Problem Types: CWE-843

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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Hardware	Netapp	8300	-	All	All	All
Operating System	Netapp	8300 Firmware	-	All	All	All
Hardware	Netapp	8700	-	All	All	All
Operating System	Netapp	8700 Firmware	-	All	All	All
Hardware	Netapp	A400	-	All	All	All
Operating System	Netapp	A400 Firmware	-	All	All	All
Hardware	Netapp	A700s	-	All	All	All
Operating System	Netapp	A700s Firmware	-	All	All	All
Hardware	Netapp	C400	-	All	All	All
Operating System	Netapp	C400 Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All

Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link	Tags
kernel/git/next/linux-next.git - The linux-next integration testing tree	MISC	git.kernel.org	
[SECURITY] [DLA 3404-1] linux-5.10 security update	MLIST	lists.debian.org	
[debian-lts-announce] 20240111 [SECURITY] [DLA 3710-1] linux security update		lists.debian.org	Mailing List
CVE-2023-1077 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161334 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12110)
161343 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12150)
181765 Debian Security Update for linux-5.10 (DLA 3404-1)
182861 Debian Security Update for linux (CVE-2023-1077)
199298 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6033-1)
199424 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6172-1)
199425 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6171-1)
199438 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-6187-1)
199439 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6185-1)
199451 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6207-1)
199463 Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-6223-1)
199465 Ubuntu Security Notification for Linux kernel (Xilinx ZynqMP) Vulnerabilities (USN-6222-1)
199614 Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6256-1)

354820 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-043
354822 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-015
354837 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-028
354882 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-121
354886 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-119
354887 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-120
355138 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355228 Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-003
355288 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355291 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355297 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355301 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355305 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355307 Amazon Linux Security Advisory for kernel : ALAS-2023-138
355314 Amazon Linux Security Advisory for kernel : ALAS2023-2023-138
378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
378701 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0030)
378710 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
390294 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2024-0002)
6000429 Debian Security Update for linux (DLA 3710-1)
6140212 AWS Bottlerocket Security Update for kernel (GHSA-4xgc-9m6g-cc55)
754106 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2534-1)
754160 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2808-1)
754167 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2822-1)
754170 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2834-1)
754183 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2859-1)
754829 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP3) (SUSE-SU-2023:3594-1)
754830 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 15 SP1) (SUSE-SU-2023:3596-1)

754831	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP3) (SUSE-SU-2023:3595-1)
754834	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 25 for SLE 15 SP3) (SUSE-SU-2023:3607-1)
754835	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 15 SP1) (SUSE-SU-2023:3603-1)
754839	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 15 SP2) (SUSE-SU-2023:3621-1)
754840	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 15 SP2) (SUSE-SU-2023:3620-1)
754841	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP3) (SUSE-SU-2023:3623-1)
754842	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 35 for SLE 15 SP2) (SUSE-SU-2023:3612-1)
754844	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 32 for SLE 15 SP3) (SUSE-SU-2023:3628-1)
754845	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP3) (SUSE-SU-2023:3627-1)
754847	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP3) (SUSE-SU-2023:3631-1)
754848	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2023:3630-1)
754852	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 12 for SLE 15 SP4) (SUSE-SU-2023:3648-1)
754853	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP4) (SUSE-SU-2023:3647-1)
754854	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 8 for SLE 15 SP4) (SUSE-SU-2023:3644-1)
754859	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP4) (SUSE-SU-2023:3657-1)
754872	SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 7 for SLE 15 SP4) (SUSE-SU-2023:3675-1)
754873	SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2023:3671-1)
754874	SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 6 for SLE 15 SP4) (SUSE-SU-2023:3668-1)
755851	SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)

© [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](#)