



CVE-2023-0045

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

Summary

CVE	CVE-2023-0045
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-25 23:15:00 UTC
Updated	2023-08-11 19:53:00 UTC
Description	The current implementation of the prctl syscall does not issue an IBPB immediately during the syscall. The ib_prctl_set fun

Risk And Classification

Problem Types: CWE-610

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
Application	Netapp	Active Iq Unified Manager	-	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
Linux Kernel: Bypassing Spectre-BTI User Space Mitigations · Advisory · google/security-research · GitHub	MISC	github.com

403 Forbidden	MISC	security.netapp.co
kernel/git/tip/tip.git - Unnamed repository; edit this file 'description' to name the repository.	MISC	git.kernel.org
[SECURITY] [DLA 3403-1] linux security update	MISC	lists.debian.org
[SECURITY] [DLA 3404-1] linux-5.10 security update	MISC	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181765 Debian Security Update for linux-5.10 (DLA 3404-1)
181768 Debian Security Update for linux (DLA 3403-1)
183815 Debian Security Update for linux (CVE-2023-0045)
199207 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5914-1)
199208 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5915-1)
199210 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5913-1)
199212 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5917-1)
199218 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5927-1)
199224 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5934-1)
199226 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5939-1)
199230 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5940-1)
199239 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5951-1)
199251 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5970-1)
199258 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5979-1)
199260 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5982-1)
199261 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5984-1)
199265 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5987-1)
199267 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5991-1)
199276 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6000-1)
199280 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6004-1)

199300 Ubuntu Security Notification for Linux kernel (Qualcomm Snapdragon) Vulnerabilities (USN-6030-1)
199502 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5975-1)
199541 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5924-1)
199555 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5926-1)
199570 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5981-1)
199587 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6009-1)
199590 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-5884-1)
354775 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-042
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)
379043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
673005 EulerOS Security Update for kernel (EulerOS-SA-2023-1873)
673017 EulerOS Security Update for kernel (EulerOS-SA-2023-1978)
673047 EulerOS Security Update for kernel (EulerOS-SA-2023-1956)
673121 EulerOS Security Update for kernel (EulerOS-SA-2023-2296)
673157 EulerOS Security Update for kernel (EulerOS-SA-2023-2272)
753743 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0618-1)
753745 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0634-1)
753807 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0768-1)
753808 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0778-1)
753810 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0780-1)
753832 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0852-1)
755842 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:0774-1)
755851 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)
755900 SUSE Enterprise Linux Security Update for the Linux-RT Kernel (SUSE-SU-2023:0488-1)

© 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](#)