



CVE-2022-1882

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

Summary

CVE	CVE-2022-1882
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-26 17:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	A use-after-free flaw was found in the Linux kernel's pipes functionality in how a user performs manipulations with the pipe

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.18	rc1	All	All
Operating System	Linux	Linux Kernel	5.18	rc2	All	All
Operating System	Linux	Linux Kernel	5.18	rc3	All	All
Operating System	Linux	Linux Kernel	5.18	rc4	All	All
Operating System	Linux	Linux Kernel	5.18	rc5	All	All
Operating System	Linux	Linux Kernel	5.18	rc6	All	All
Operating System	Linux	Linux Kernel	5.18	rc7	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e 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	H500e	-	All	All	All

Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source
[PATCH] fs/pipe: Deinitialize the watch_queue when pipe is freed	MISC
[PATCH] fs/pipe: Deinitialize the watch_queue when pipe is freed	
CVE-2022-1882 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM
2089701 – (CVE-2022-1882) CVE-2022-1882 kernel: Use-After-Free in free_pipe_info() could cause an escalation of privileges	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160583 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2458)
180956 Debian Security Update for linux (CVE-2022-1882)
198979 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5667-1)
198989 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5683-1)
199009 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5703-1)
241417 Red Hat Update for kernel security (RHSA-2023:2458)
241468 Red Hat Update for kernel-rt (RHSA-2023:2148)
752850 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2022:4035-1)
752875 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 2 for SLE 15 SP4) (SUSE-SU-2022:4039-1)
752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)
752913 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)
752930 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:4113-1)

753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
902134 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9841)
902139 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9844)
902463 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10120)
902465 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10101)
902510 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10118)
902517 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10105)
904182 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10118-1)
904270 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10105-1)
905872 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10118-2)
906491 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10105-2)
941023 AlmaLinux Security Update for kernel (ALSA-2023:2458)
941061 AlmaLinux Security Update for kernel-rt (ALSA-2023:2148)

© [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](#)