Linux Kernel Improper Ownership Management Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-0386
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 21:15:00 UTC
Updated	2023-06-26 16:56:00 UTC
Description	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was fou

Risk And Classification

EPSS: 0.543220000 probability, percentile 0.980410000 (date 2026-05-09)

CISA KEV: Listed on 2025-06-17; due 2025-07-08; ransomware use Unknown

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Improper Ownership Management Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. For more information, please see: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a ; https://access.redhat.com/security/cve/cve-2023-0386 ; https://security.netapp.com/advisory/ntap-20230420-0004/ ; https://nvd.nist.gov/vuln/detail/CVE-2023-0386

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	6.2	rc1	All	All
Operating System	Linux	Linux Kernel	6.2	rc2	All	All
Operating System	Linux	Linux Kernel	6.2	rc3	All	All

Operating System	Linux	Linux Kernel	6.2	rc4	All	All
Operating System	Linux	Linux Kernel	6.2	rc5	All	All

References

Reference	Source	Link	Tags
Kernel Live Patch Security Notice LSN-0095-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
[SECURITY] [DLA 3446-1] linux-5.10 security update	MLIST	lists.debian.org	
CVE-2023-0386 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
Debian -- Security Information -- DSA-5402-1 linux	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160537 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-1566)

160546 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-1703)

181781 Debian Security Update for linux (DSA 5402-1)

181828 Debian Security Update for linux-5.10 (DLA 3446-1)

183291 Debian Security Update for linux (CVE-2023-0386)

199292 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6025-1)

199303 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6040-1)

199306 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6043-1)

199321 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6057-1)

199330 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6072-1)

199334 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6071-1)

199385 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6134-1)

241305 Red Hat Update for kernel security (RHSA-2023:1554)

241310 Red Hat Update for kernel-rt (RHSA-2023:1584)

241324 Red Hat Update for kernel security (RHSA-2023:1566)

241328 Red Hat Update for kpatch-patch (RHSA-2023:1659)

241329 Red Hat Update for kpatch-patch (RHSA-2023:1660)

241334 Red Hat Update for kpatch-patch (RHSA-2023:1681)

241336 Red Hat Update for kernel-rt (RHSA-2023:1691)

241337 Red Hat Update for kernel (RHSA-2023:1703)

241379 Red Hat Update for kernel (RHSA-2023:1970)

241381 Red Hat Update for kpatch-patch (RHSA-2023:1984)

241394 Red Hat Update for kernel-rt (RHSA-2023:1980)

378537 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0048)

378710 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)

906846 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25742-1)

907052 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25752-1)

907121 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (25904-1)

940970 AlmaLinux Security Update for kernel (ALSA-2023:1566)

940974 AlmaLinux Security Update for kernel-rt (ALSA-2023:1584)

940982 AlmaLinux Security Update for kernel (ALSA-2023:1703)

940991 AlmaLinux Security Update for kernel-rt (ALSA-2023:1691)

960903 Rocky Linux Security Update for kernel (RLSA-2023:1566)

960918 Rocky Linux Security Update for kernel-rt (RLSA-2023:1584)

© 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 registred 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**