



# CVE-2023-0458

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

## Summary

<b>CVE</b>	CVE-2023-0458
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-26 19:15:00 UTC
<b>Updated</b>	2023-05-09 13:58:00 UTC
<b>Description</b>	A speculative pointer dereference problem exists in the Linux Kernel on the do_prlimit() function. The resource argument va

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.2	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.2	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.2	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.2	rc4	All	All

## References

Reference	Source	Link	Tags
<a href="#">kernel/git/stable/linux.git - Linux kernel stable tree</a>	MISC	<a href="#">git.kernel.org</a>	
<a href="#">[SECURITY] [DLA 3403-1] linux security update</a>	MISC	<a href="#">lists.debian.org</a>	
<a href="#">prlimit: do_prlimit needs to have a speculation check · torvalds/linux@7397906 · GitHub</a>	MISC	<a href="#">github.com</a>	
<a href="#">[SECURITY] [DLA 3404-1] linux-5.10 security update</a>	MISC	<a href="#">lists.debian.org</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160719](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12375)

[160837](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-4377)

[161147](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)

[181765](#) Debian Security Update for linux-5.10 (DLA 3404-1)

[181768](#) Debian Security Update for linux (DLA 3403-1)

[184967](#) Debian Security Update for linux (CVE-2023-0458)

[199343](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6079-1)

[199353](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6091-1)

[199354](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6096-1)

[199356](#) Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6093-1)

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

[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)

[199617](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6254-1)

[199764](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6385-1)

[199775](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6341-1)

[241878](#) Red Hat Update for kernel security (RHSA-2023:4377)

[241886](#) Red Hat Update for kernel-rt (RHSA-2023:4378)

[242434](#) Red Hat Update for kernel-rt security (RHSA-2023:6901)

[242451](#) Red Hat Update for kernel security (RHSA-2023:7077)

[242789](#) Red Hat Update for kernel (RHSA-2024:0575)

[242890](#) Red Hat Update for kernel (RHSA-2024:0724)

[355255](#) Amazon Linux Security Advisory for kernel : ALAS-2023-127

[355287](#) Amazon Linux Security Advisory for kernel : ALAS-2023-127

[355294](#) Amazon Linux Security Advisory for kernel : ALAS-2023-127

[355295](#) Amazon Linux Security Advisory for kernel : ALAS-2023-127

[355300](#) Amazon Linux Security Advisory for kernel : ALAS-2023-127

355303 Amazon Linux Security Advisory for kernel : ALAS-2023-127
355309 Amazon Linux Security Advisory for kernel : ALAS-2023-127
355312 Amazon Linux Security Advisory for kernel : ALAS2023-2023-127
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)
390285 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2023-0017)
390286 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2023-0018)
390292 Oracle Managed Virtualization (VM) Server for x86 Security Update for None (OVMSA-2023-0016)
673214 EulerOS Security Update for kernel (EulerOS-SA-2023-2383)
673232 EulerOS Security Update for kernel (EulerOS-SA-2023-2357)
673261 EulerOS Security Update for kernel (EulerOS-SA-2023-2614)
673272 EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
673393 EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
673498 EulerOS Security Update for kernel (EulerOS-SA-2023-3132)
674113 EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
906883 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26412-1)
906930 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26415-1)
941213 AlmaLinux Security Update for kernel (ALSA-2023:4377)
941214 AlmaLinux Security Update for kernel-rt (ALSA-2023:4378)
941453 AlmaLinux Security Update for kernel (ALSA-2023:7077)
960961 Rocky Linux Security Update for kernel-rt (RLSA-2023:4378)

© [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](#)**