



# CVE-2023-32250

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

## Summary

<b>CVE</b>	CVE-2023-32250
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-10 16:15:00 UTC
<b>Updated</b>	2023-11-07 04:14:00 UTC
<b>Description</b>	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

## References

Reference
ZDI-23-698   Zero Day Initiative
2208849 – (CVE-2023-32250, ZDI-23-698, ZDI-CAN-20481) CVE-2023-32250 kernel: ksmbd: session race condition remote code execution v
July 2023 Linux Kernel 6.4 Vulnerabilities in NetApp Products   NetApp Product Security
cve-details
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

199421 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6173-1)
200100 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6626-1)
200100 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6626-1)

<a href="#">200103</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-1)
<a href="#">200111</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6626-2)
<a href="#">200118</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-2)
<a href="#">200120</a> Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6626-3)
<a href="#">6000207</a> Debian Security Update for linux (DSA 5448-1)
<a href="#">907108</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27401-1)
<a href="#">907145</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27399-1)
<a href="#">907859</a> Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (27641-1)

© [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](#)**