



CVE-2021-45100

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

Summary

CVE	CVE-2021-45100
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-16 05:15:00 UTC
Updated	2022-03-29 16:28:00 UTC
Description	The ksmbd server through 3.4.2, as used in the Linux kernel through 5.15.8, sometimes communicates in cleartext even th

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ksmbd Project	Ksmbd	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	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						
CVE-2021-45100 Linux Kernel Vulnerability in NetApp Products NetApp Product Security						
'Re: [PATCH] ksmbd: disable SMB2_GLOBAL_CAP_ENCRYPTION for SMB 3.1.1' - MARC						
Plaintext connection despite encryption enabled · Issue #550 · cifs-team/ksmbd · GitHub						
Do not set SMB2_GLOBAL_CAP_ENCRYPTION for SMB 3.1.1. Fixes #550 by socram8888 · Pull Request #551 · cifs-team/ksmbd · GitHub						
CVE Program record						
NVD vulnerability detail						
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
183829 Debian Security Update for linux (CVE-2021-45100)						

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)