



CVE-2021-3501

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

Summary

CVE	CVE-2021-3501
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-06 13:15:00 UTC
Updated	2022-05-13 20:52:00 UTC
Description	A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an e

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Cloud Backup	-	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
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time	8	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv	8	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.4	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[CVE-2021-3501 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security](#)

[1950136 – \(CVE-2021-3501\) CVE-2021-3501 kernel: userspace applications can misuse the KVM API to cause a write of 16 bytes at an offset](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159239](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-2168)

[180455](#) Debian Security Update for linux (CVE-2021-3501)

[198396](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4977-1)

[198402](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4983-1)

[239379](#) Red Hat Update for kernel (RHSA-2021:2168)

[239448](#) Red Hat Update for kpatch-patch (RHSA-2021:2165)

[239454](#) Red Hat Update for kernel-rt (RHSA-2021:2169)

[353159](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-001

[6140243](#) AWS Bottlerocket Security Update for kernel (GHSA-57hf-5hq2-ff32)

[900096](#) CBL-Mariner Linux Security Update for kernel 5.10.52.1

900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901036 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6569-1)
903061 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4184)
906199 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4184-1)
940125 AlmaLinux Security Update for kernel (ALSA-2021:2168)
960066 Rocky Linux Security Update for kernel (RLSA-2021:2168)

© [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](#)