



CVE-2021-28038

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

Summary

CVE	CVE-2021-28038
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-05 18:15:00 UTC
Updated	2023-08-22 14:25:00 UTC
Description	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.12	rc1	All	All
Operating System	Linux	Linux Kernel	5.12	rc2	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Operating System	Xen	Xen	-	All	All	All
Operating System	Xen	Xen	-	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 2586-1] linux security update	MLIST	lists.debian
oss-security - Xen Security Advisory 367 v2 (CVE-2021-28038) - Linux: netback fails to honor grant mapping errors	MLIST	www.open
XSA-367 - Xen Security Advisories	MISC	xenbits.xe
[SECURITY] [DLA 2610-1] linux-4.19 security update	MLIST	lists.debian
March 2021 Linux Kernel 5.11.3 Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.ne

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159157](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9172)

[159158](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9175)

[159175](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9215)

[159177](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9220)

[159178](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9221)

[174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)

[174897](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)

[174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

[174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

[178507](#) Debian Security Update for linux-4.19 (DLA 2610-1)

[180534](#) Debian Security Update for linux (CVE-2021-28038)

[198323](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4904-1)

[198327](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4911-1)

[198363](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4945-1)

[198371](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4946-1)

[198377](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) vulnerabilities (USN-4945-2)

[198403](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4984-1)

[352244](#) Amazon Linux Security Advisory for kernel: ALAS-2021-1487

[352254](#) Amazon Linux Security Advisory for kernel: ALAS2-2021-1616

[353100](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-024

[353101](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

[353102](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026

[353150](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-001

375504 Citrix XenServer Security Updates(CTX306565)
390225 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0016)
6140286 AWS Bottlerocket Security Update for kernel (GHSA-7xrx-wcv2-9h2m)
750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)
750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
750199 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750276 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)
750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

© [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](#)