



# CVE-2022-3643

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

## Summary

<b>CVE</b>	CVE-2022-3643
<b>State</b>	PUBLIC
<b>Assigner</b>	security@xen.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-07 01:15:00 UTC
<b>Updated</b>	2023-11-29 15:15:00 UTC
<b>Description</b>	Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort

## Risk And Classification

**Problem Types:** CWE-74

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Broadcom</a>	<a href="#">Bcm5780</a>	-	All	All	All
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

## References

Reference	Source
[SECURITY] [DLA 3245-1] linux security update	MLIST
Kernel Live Patch Security Notice LSN-0099-1 ≈ Packet Storm	
oss-security - Xen Security Advisory 423 v2 (CVE-2022-3643) - Guests can trigger NIC interface reset/abort/crash via netback	MLIST
[SECURITY] [DLA 3244-1] linux-5.10 security update	MLIST
<a href="https://xenbits.xenproject.org/xsa/advisory-423.txt">xenbits.xenproject.org/xsa/advisory-423.txt</a>	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">181438</a> Debian Security Update for linux (CVE-2022-3643)
<a href="#">181440</a> Debian Security Update for linux-5.10 (DLA 3244-1)
<a href="#">181565</a> Debian Security Update for linux (DLA 3245-1)
<a href="#">199103</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5803-1)
<a href="#">199105</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5804-1)
<a href="#">199106</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5804-2)
<a href="#">199111</a> Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5808-1)
<a href="#">199118</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5814-1)
<a href="#">199121</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5813-1)
<a href="#">199132</a> Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5829-1)
<a href="#">199136</a> Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5831-1)
<a href="#">199137</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5830-1)
<a href="#">199138</a> Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5832-1)
<a href="#">199160</a> Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5860-1)
<a href="#">199165</a> Ubuntu Security Notification for Linux kernel (Dell300x) Vulnerabilities (USN-5861-1)
<a href="#">199179</a> Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5877-1)
<a href="#">199180</a> Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5875-1)
<a href="#">199183</a> Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5879-1)
<a href="#">199213</a> Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-5918-1)
<a href="#">199490</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5802-1)
<a href="#">199519</a> Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5863-1)
<a href="#">199547</a> Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-5794-1)
<a href="#">354668</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-025
<a href="#">354669</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-012
<a href="#">354670</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-041
<a href="#">354736</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-1932
<a href="#">354842</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1706
<a href="#">355199</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
<a href="#">373400</a> Alibaba Cloud Linux Security Update for cloud kernel (ALINUX-SA-2023040)

<a href="#">378468</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
<a href="#">378512</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
<a href="#">379435</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)
<a href="#">6140027</a> AWS Bottlerocket Security Update for kernel (GHSA-qgmh-8q8r-6p7p)
<a href="#">6140061</a> AWS Bottlerocket Security Update for kernel (GHSA-qgmh-8q8r-6p7p)
<a href="#">753014</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4505-1)
<a href="#">753020</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4585-1)
<a href="#">753034</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4504-1)
<a href="#">753038</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)
<a href="#">753039</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4574-1)
<a href="#">753047</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4566-1)
<a href="#">753060</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4615-1)
<a href="#">753063</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
<a href="#">753562</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0134-1)
<a href="#">753583</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0152-1)
<a href="#">753688</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0406-1)
<a href="#">904975</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.79.1-1.cm2 (12545)
<a href="#">904995</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.80.1-1.cm2 (12550)
<a href="#">905010</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.81.1-1.cm2 (12552)
<a href="#">905045</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.74.1-1.cm2 (12538)
<a href="#">905047</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.72.1-1.cm2 (12533)
<a href="#">905082</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.48.1-4.cm2 (12521)
<a href="#">905134</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.82.1-1.cm2 (12556)
<a href="#">905147</a> Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.77.1-1.cm2 (12539)

© [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](#).

