



# CVE-2021-28714

Published on: 01/06/2022 12:00:00 AM UTC

Last Modified on: 08/08/2023 02:22:00 PM UTC

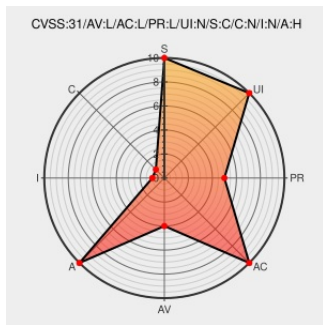
## CVE-2021-28714

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some

measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714)

CVE-2021-28714 has been assigned by [security@xen.org](mailto:security@xen.org) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Linux](#) - Linux version ? **consult Xen advisory XSA-392**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>NONE</b>	<b>NONE</b>	<b>HIGH</b>

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
<b>LOCAL</b>	<b>LOW</b>	<b>NONE</b>

<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
<b>NONE</b>	<b>NONE</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
[SECURITY] [DLA 2941-1] linux-4.19 security update	<a href="https://lists.debian.org">lists.debian.org</a> <a href="#">text/html</a>	<a href="#">@ MLIST [debian-lts-announce] 20220309 [SECURITY] [DLA 2941-1] linux-4.19 security update</a>
[SECURITY] [DLA 2940-1] linux security update	<a href="https://lists.debian.org">lists.debian.org</a> <a href="#">text/html</a>	<a href="#">@ MLIST [debian-lts-announce] 20220309 [SECURITY] [DLA 2940-1] linux security update</a>
	<a href="https://xenbits.xenproject.org">xenbits.xenproject.org</a> <a href="#">text/plain</a>	<a href="https://xenbits.xenproject.org/xsa/advisory-392.txt">✖ MISC xenbits.xenproject.org/xsa/advisory-392.txt</a>
Debian -- Security Information -- DSA-5050-1 linux	<a href="https://www.debian.org">www.debian.org</a> <b>Deprecated Link</b> <a href="#">text/html</a>	<a href="#">@ DEBIAN DSA-5050</a>
Debian -- Security Information -- DSA-5096-1 linux	<a href="https://www.debian.org">www.debian.org</a> <b>Deprecated Link</b> <a href="#">text/html</a>	<a href="#">@ DEBIAN DSA-5096</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

- [179012](#) Debian Security Update for linux (DSA 5050-1)
- [179117](#) Debian Security Update for linux (DSA 5096-1)
- [179118](#) Debian Security Update for linux (DLA 2940-1)
- [179119](#) Debian Security Update for linux-4.19 (DLA 2941-1)
- [183448](#) Debian Security Update for linux (CVE-2021-28714)
- [198659](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5278-1)
- [198678](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5298-1)
- [198708](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5337-1)
- [198709](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5338-1)
- [198731](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5368-1)
- [198740](#) Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-5377-1)
- [282190](#) Fedora Security Update for kernel (FEDORA-2021-e6cbca1e9e)
- [282191](#) Fedora Security Update for kernel (FEDORA-2021-4f1a2cdf2e)
- [353130](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-021
- [353151](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-009

- [353160](#) Amazon Linux Security Advisory for kernel : ALAS2-2022-1749
- [353161](#) Amazon Linux Security Advisory for kernel : ALAS-2022-1563
- [353242](#) Amazon Linux Security Advisory for kernel : ALAC2012-2022-036
- [353243](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037
- [353244](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038
- [354747](#) Amazon Linux Security Advisory for kernel : ALAS-2023-1688
- [376925](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)
- [671505](#) EulerOS Security Update for kernel (EulerOS-SA-2022-1489)
- [751590](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0056-1)
- [751600](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0068-1)
- [751602](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)
- [751622](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0131-1)
- [751654](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)
- [751695](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)
- [751697](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)
- [751701](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0366-1)
- [751702](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0371-1)
- [751989](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0131-1)
- [753133](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0181-1)
- [753264](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0079-1)
- [753355](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0056-1)
- [900519](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (7165)
- [905757](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (7165-1)

#### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:						

cpe:2.3:o:linux:linux\_kernel:\*.:.:.:.:.:.:.:.:.:.:

## Social Mentions

Source	Title	Posted (UTC)
 @oss_security	Xen Security Advisory 392 v4 (CVE-2021-28714,CVE-2021-28715) - Guest can force Linux netback driver to hog large am... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-12-20 16:31:13
 @CVEreport	CVE-2021-28714 : Guest can force #Linux netback driver to hog large amounts of #kernel memory T[his CNA informatio... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-01-06 17:14:05

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)