



# CVE-2022-1012

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

## Summary

<b>CVE</b>	CVE-2022-1012
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-05 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:41:00 UTC
<b>Description</b>	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table pertu

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.18	rc5	All	All

## References

### Reference

- 2064604 – (CVE-2022-1012) CVE-2022-1012 kernel: Small table perturb size in the TCP source port generation algorithm can lead to informa
- [PATCH net 0/7] insufficient TCP source port randomness
- [PATCH net 0/7] insufficient TCP source port randomness
- CVE-2022-1012 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security
- Diff - b2d057560b8107c633b39aabe517ff9d93f285e3^! - pub/scm/linux/kernel/git/jkirsher/net-queue - Git at Google
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159931</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5249)
<a href="#">160028</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5819)
<a href="#">179371</a> Debian Security Update for linux (DSA 5161-1)
<a href="#">180282</a> Debian Security Update for linux (DLA 3065-1)
<a href="#">180605</a> Debian Security Update for linux (DSA 5173-1)
<a href="#">180864</a> Debian Security Update for linux (CVE-2022-1012)
<a href="#">198823</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5471-1)
<a href="#">198921</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5594-1)
<a href="#">198927</a> Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-5599-1)
<a href="#">198929</a> Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5602-1)
<a href="#">198942</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5616-1)
<a href="#">198949</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5622-1)
<a href="#">198950</a> Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5623-1)
<a href="#">198954</a> Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5630-1)
<a href="#">198962</a> Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5639-1)
<a href="#">198966</a> Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5647-1)
<a href="#">198970</a> Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5654-1)
<a href="#">198974</a> Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5660-1)
<a href="#">198978</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5669-1)
<a href="#">198985</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5678-1)
<a href="#">198994</a> Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5687-1)
<a href="#">240487</a> Red Hat Update for kpatch-patch (RHSA-2022:5214)
<a href="#">240494</a> Red Hat Update for kernel (RHSA-2022:5220)
<a href="#">240499</a> Red Hat Update for kernel (RHSA-2022:5249)
<a href="#">240527</a> Red Hat Update for kernel-rt (RHSA-2022:5267)

<a href="#">240531</a> Red Hat Update for kernel-rt (RHSA-2022:5224)
<a href="#">240544</a> Red Hat Update for kernel-rt (RHSA-2022:5633)
<a href="#">240545</a> Red Hat Update for kernel (RHSA-2022:5626)
<a href="#">240581</a> Red Hat Update for kernel-rt (RHSA-2022:5834)
<a href="#">240594</a> Red Hat Update for kernel (RHSA-2022:5819)
<a href="#">353976</a> Amazon Linux Security Advisory for kernel : ALAS-2022-1604
<a href="#">353985</a> Amazon Linux Security Advisory for kernel : ALAS2-2022-1813
<a href="#">353993</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-016
<a href="#">353994</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-028
<a href="#">354007</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-015
<a href="#">354008</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-030
<a href="#">354017</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-032
<a href="#">354023</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-017
<a href="#">377117</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)
<a href="#">377871</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)
<a href="#">6140257</a> AWS Bottlerocket Security Update for kernel (GHSA-g9px-j6j3-h52v)
<a href="#">671929</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1999)
<a href="#">672003</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2134)
<a href="#">672017</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2244)
<a href="#">672045</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2225)
<a href="#">752340</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2377-1)
<a href="#">752349</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2382-1)
<a href="#">752364</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2422-1)
<a href="#">752370</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
<a href="#">752391</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2549-1)
<a href="#">752615</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3408-1)
<a href="#">752632</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3450-1)
<a href="#">753091</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2172-1)
<a href="#">753148</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)

753271 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2424-1)
902670 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10472)
902671 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10468)
903970 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10472-1)
904160 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10468-1)
906064 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10472-2)
906250 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10468-2)
940602 AlmaLinux Security Update for kernel-rt (ALSA-2022:5834)
940612 AlmaLinux Security Update for kernel (ALSA-2022:5819)
940618 AlmaLinux Security Update for kernel (ALSA-2022:5249)
940638 AlmaLinux Security Update for kernel-rt (ALSA-2022:5267)

© [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](#)**