



# CVE-2021-3573

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

## Summary

<b>CVE</b>	CVE-2021-3573
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-13 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:38:00 UTC
<b>Description</b>	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioctl

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
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>	5.13	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc4	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

Reference	Source	Link	T
oss-security - CVE-2021-3573: UAF in hci_sock_bound_ioctl() function	MISC	<a href="http://www.openwall.com">www.openwall.com</a>	
oss-security - CVE-2023-3439: Linux MCTP use-after-free in mctp_sendmsg	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
kernel/git/bluetooth/bluetooth.git - Bluetooth kernel tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
1966578 – (CVE-2021-3573) CVE-2021-3573 kernel: use-after-free in function hci_sock_bound_ioctl()	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159393](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9450)

[159394](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9451)

[159402](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9458)

[159404](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9460)

[159424](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9485)

[159427](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9488)

[159492](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)

[159664](#) Oracle Enterprise Linux Security Update for kernel security and bug fix update (ELSA-2022-0620)

[159777](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9348)

[178679](#) Debian Security Update for linux-4.19 (DLA 2690-1)

[178680](#) Debian Security Update for linux (DLA 2689-1)

[180145](#) Debian Security Update for linux (CVE-2021-3573)

[198436](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5015-1) (Sequoia)

[198463](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5044-1)

[198464](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5045-1)

[198465](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5046-1)

[198468](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5050-1)

[239816](#) Red Hat Update for kernel security (RHSA-2021:4356)

[239879](#) Red Hat Update for kernel-rt (RHSA-2021:4140)

[240096](#) Red Hat Update for kernel-rt (RHSA-2022:0622)

[240115](#) Red Hat Update for kernel (RHSA-2022:0620)

[257155](#) CentOS Security Update for kernel (CESA-2022:0620)

[281633](#) Fedora Security Update for kernel (FEDORA-2021-db2bb87f35)

[281634](#) Fedora Security Update for kernel (FEDORA-2021-bc2a819bc5)

[282100](#) Fedora Security Update for kernel (FEDORA-2021-1000)

<a href="#">352489</a> Amazon Linux Security Advisory for kernel: ALAS2-2021-1685
<a href="#">352831</a> Amazon Linux Security Advisory for kernel: ALAC2012-2021-030
<a href="#">352832</a> Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-031
<a href="#">352833</a> Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-032
<a href="#">353147</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004
<a href="#">353158</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002
<a href="#">390261</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2022-0014)
<a href="#">670578</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2336)
<a href="#">670634</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2392)
<a href="#">671047</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2588)
<a href="#">750828</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2305-1)
<a href="#">750842</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2352-1)
<a href="#">751238</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2021:3459-1)
<a href="#">900316</a> CBL-Mariner Linux Security Update for kernel 5.10.57.1
<a href="#">900319</a> CBL-Mariner Linux Security Update for kernel 5.10.60.1
<a href="#">901114</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6574-1)
<a href="#">903578</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5421)
<a href="#">905736</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5421-1)
<a href="#">940265</a> AlmaLinux Security Update for kernel (ALSA-2021:4356)
<a href="#">960044</a> Rocky Linux Security Update for kernel (RLSA-2021:4356)
<a href="#">960065</a> Rocky Linux Security Update for kernel-rt (RLSA-2021:4140)

© [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](#)**