CVE-2021-3573

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.13	rc1	All	All
Operating System	Linux	Linux Kernel	5.13	rc2	All	All
Operating System	Linux	Linux Kernel	5.13	rc3	All	All
Operating System	Linux	Linux Kernel	5.13	rc4	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

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

NVD vulnerability detail NVD nvd.nist.gov 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)

352489 Amazon Linux Security Advisory for kernel: ALAS2-2021-1685

352831 Amazon Linux Security Advisory for kernel: ALAC2012-2021-030

352832 Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-031

352833 Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-032

353147 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004

353158 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002

390261 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2022-0014)

670578 EulerOS Security Update for kernel (EulerOS-SA-2021-2336)

670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

750828 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2305-1)

750842 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2352-1)

751238 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2021:3459-1)

900316 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

901114 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6574-1)

903578 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5421)

905736 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5421-1)

940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)

960044 Rocky Linux Security Update for kernel (RLSA-2021:4356)

960065 Rocky Linux Security Update for kernel-rt (RLSA-2021:4140)