CVE-2021-3564

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3564
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-08 12:15:00 UTC
Updated	2023-02-12 23:41:00 UTC
Description	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user atta

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
oss-security - CVE-2021-3564 Linux Bluetooth device initialization implementation bug	MLIST
oss-security - Re: CVE-2021-3564 Linux Bluetooth device initialization implementation bug	MLIST
[SECURITY] [DLA 2689-1] linux security update	MLIST
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
oss-security - CVE-2021-3564 Linux Bluetooth device initialization implementation bug	MISC
1964139 – (CVE-2021-3564) CVE-2021-3564 kernel: double free in bluetooth subsystem when the HCI device initialization fails	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159338 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9404)
- 159339 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9406)
- 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)
- 159453 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9534)
- 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)
- 178679 Debian Security Update for linux-4.19 (DLA 2690-1)
- 178680 Debian Security Update for linux (DLA 2689-1)
- 179885 Debian Security Update for linux (CVE-2021-3564)
- 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)
- 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

390250 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0036)

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

670744 EulerOS Security Update for kernel (EulerOS-SA-2021-2502)

670772 EulerOS Security Update for kernel (EulerOS-SA-2021-2530)

670796 EulerOS Security Update for kernel (EulerOS-SA-2021-2554)

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

751695 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)

751696 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0364-1)

751697 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)

751698 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)

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)

751703 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0372-1)

900084 CBL-Mariner Linux Security Update for kernel 5.10.52.1

900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

901135 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6573-1)

903647 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4356)

905740 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4356-1)

906341 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6573-2)

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

CVE.report and Source URL Uptime Status status.cve.report