



CVE-2020-26558

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

Summary

CVE	CVE-2020-26558
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-24 18:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-r

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bluetooth	Bluetooth Core Specification	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Hardware	Intel	Ac 1550	-	All	All	All
Operating System	Intel	Ac 1550 Firmware	-	All	All	All
Hardware	Intel	Ac 3165	-	All	All	All
Operating System	Intel	Ac 3165 Firmware	-	All	All	All
Hardware	Intel	Ac 3168	-	All	All	All
Operating System	Intel	Ac 3168 Firmware	-	All	All	All
Hardware	Intel	Ac 7265	-	All	All	All
Operating System	Intel	Ac 7265 Firmware	-	All	All	All
Hardware	Intel	Ac 8260	-	All	All	All
Operating System	Intel	Ac 8260 Firmware	-	All	All	All
Hardware	Intel	Ac 8265	-	All	All	All
Operating System	Intel	Ac 8265 Firmware	-	All	All	All
Hardware	Intel	Ac 9260	-	All	All	All
Operating System	Intel	Ac 9260 Firmware	-	All	All	All

Hardware	Intel	Ac 9461	-	All	All	All
Operating System	Intel	Ac 9461 Firmware	-	All	All	All
Hardware	Intel	Ac 9462	-	All	All	All
Operating System	Intel	Ac 9462 Firmware	-	All	All	All
Hardware	Intel	Ac 9560	-	All	All	All
Operating System	Intel	Ac 9560 Firmware	-	All	All	All
Hardware	Intel	Ax1650	-	All	All	All
Operating System	Intel	Ax1650 Firmware	-	All	All	All
Hardware	Intel	Ax1675	-	All	All	All
Operating System	Intel	Ax1675 Firmware	-	All	All	All
Hardware	Intel	Ax200	-	All	All	All
Operating System	Intel	Ax200 Firmware	-	All	All	All
Hardware	Intel	Ax201	-	All	All	All
Operating System	Intel	Ax201 Firmware	-	All	All	All
Hardware	Intel	Ax210	-	All	All	All
Operating System	Intel	Ax210 Firmware	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference

VU#799380 - Devices supporting Bluetooth Core and Mesh Specifications are vulnerable to impersonation attacks and AuthValue disclosure

INTEL-SA-00520

Debian -- Security Information -- DSA-4951-1 bluez

BlueZ: Multiple Vulnerabilities (GLSA 202209-16) — Gentoo security

INTEL-SA-00517

[SECURITY] [DLA 2689-1] linux security update

[SECURITY] [DLA 2692-1] bluez security update

[SECURITY] [DLA 2690-1] linux-4.19 security update

[SECURITY] Fedora 34 Update: kernel-5.12.7-300.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 34 Update: kernel-5.12.7-300.fc34 - package-announce - Fedora Mailing-Lists

Reporting Security Vulnerabilities | Bluetooth® Technology Website

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159514](#) Oracle Enterprise Linux Security Update for bluez (ELSA-2021-4432)

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

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

[178684](#) Debian Security Update for bluez (DLA 2692-1)

[178745](#) Debian Security Update for bluez (DSA 4951-1)

[198407](#) Ubuntu Security Notification for BlueZ vulnerabilities (USN-4989-1)

[198438](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5017-1) (Sequoia)

[198459](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, Linux-gcp, (USN-5018-1)

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

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

[239797](#) Red Hat Update for bluez (RHSA-2021:4432)

[281098](#) Fedora Security Update for kernel (FEDORA-2021-a35b44fd9f)

[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

[610344](#) Google Android Devices June 2021 Security Patch Missing

[610354](#) Google Android July 2021 Security Patch Missing for LGE

[610355](#) Google Android July 2021 Security Patch Missing for Samsung

[610358](#) Google Android July 2021 Security Patch Missing for Huawei EMUI

[610374](#) Google Android October 2021 Security Patch Missing for Huawei EMUI

[610375](#) Google Android October 2021 Security Patch Missing for Samsung

[610376](#) Google Android October 2021 Security Patch Missing for LGE

[710631](#) Gentoo Linux BlueZ Multiple Vulnerabilities (GLSA 202209-16)

[750748](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2202-1)

750750 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2184-1)
750753 OpenSUSE Security Update for bluez (openSUSE-SU-2021:2291-1)
750830 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2321-1)
750832 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2324-1)
750864 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)
750868 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2427-1)
750869 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2422-1)
750877 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2427-1)
750880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2451-1)
752696 SUSE Enterprise Linux Security Update for bluez (SUSE-SU-2022:3691-1)
752697 SUSE Enterprise Linux Security Update for bluez (SUSE-SU-2022:3687-1)
900842 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9474)
902009 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9474-1)
905824 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9474-2)

© [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](#)