



CVE-2020-24586

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

Summary

CVE	CVE-2020-24586
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-11 20:15:00 UTC
Updated	2023-04-01 22:15:00 UTC
Description	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP)

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Arista	C-200	-	All	All	All
Operating System	Arista	C-200 Firmware	All	All	All	All
Hardware	Arista	C-230	-	All	All	All
Operating System	Arista	C-230 Firmware	All	All	All	All
Hardware	Arista	C-235	-	All	All	All
Operating System	Arista	C-235 Firmware	All	All	All	All
Hardware	Arista	C-250	-	All	All	All
Operating System	Arista	C-250 Firmware	All	All	All	All
Hardware	Arista	C-260	-	All	All	All
Operating System	Arista	C-260 Firmware	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	leee	leee 802.11	All	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	All
Hardware	Intel	Ac 3168	-	All	All	All

Operating System	Intel	Ac 3168 Firmware	All	All	All	All
Hardware	Intel	Ac 7265	-	All	All	All
Operating System	Intel	Ac 7265 Firmware	All	All	All	All
Hardware	Intel	Ac 8260	-	All	All	All
Operating System	Intel	Ac 8260 Firmware	All	All	All	All
Hardware	Intel	Ac 8265	-	All	All	All
Operating System	Intel	Ac 8265 Firmware	All	All	All	All
Hardware	Intel	Ac 9260	-	All	All	All
Operating System	Intel	Ac 9260 Firmware	All	All	All	All
Hardware	Intel	Ac 9461	-	All	All	All
Operating System	Intel	Ac 9461 Firmware	All	All	All	All
Hardware	Intel	Ac 9462	-	All	All	All
Operating System	Intel	Ac 9462 Firmware	All	All	All	All
Hardware	Intel	Ac 9560	-	All	All	All
Operating System	Intel	Ac 9560 Firmware	All	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	All
Hardware	Intel	Ax201	-	All	All	All
Operating System	Intel	Ax201 Firmware	All	All	All	All
Hardware	Intel	Ax210	-	All	All	All
Operating System	Intel	Ax210 Firmware	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Linux	Mac80211	-	All	All	All

References

Reference

Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementations of 802.11 Specification Affecting Cisco Products: May 2021

FragAttacks: Security flaws in all Wi-Fi devices

Security Advisory 0063 - Arista

fragattacks/SUMMARY.md at master · vanhoefm/fragattacks · GitHub

INTEL-SA-00473

SECURITY [DL-802.11] - Intel

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

oss-security - various 802.11 security issues - fragattacks.com

[SECURITY] [DLA 3380-1] firmware-nonfree LTS new upstream version (security updates and newer firmware for Linux 5.10)

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

CVE Program record

NVD vulnerability detail



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)

[159399](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9452)

[159400](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9453)

[159403](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9459)

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

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

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

[181651](#) Debian Security Update for firmware-nonfree (DLA 3380-1)

[198416](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)

[198417](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)

[198418](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5000-1)

[198419](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5001-1)

[198425](#) Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-5000-2)

[198426](#) Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)

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

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

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

[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
390248 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)
591104 Mitsubishi Electric GT25-WLAN (Update A) Multiple Vulnerabilities (ICSA-22-102-04)
591150 Hitachi ABB Power Grids TropOS Multiple Vulnerabilities (ICSA-21-236-01,9AKK107992A4463)
670772 EulerOS Security Update for kernel (EulerOS-SA-2021-2530)
670796 EulerOS Security Update for kernel (EulerOS-SA-2021-2554)
671051 EulerOS Security Update for kernel (EulerOS-SA-2021-2663)
671441 EulerOS Security Update for kernel (EulerOS-SA-2022-1366)
671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)
750117 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1891-1)
750118 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1890-1)
750121 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1888-1)
750125 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1887-1)
750126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1889-1)
750139 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1913-1)
750140 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1912-1)
750171 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0843-1)
750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750741 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0947-1)
750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
750864 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)
750880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2451-1)
940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)

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](#)