



CVE-2020-26147

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

Summary

CVE	CVE-2020-26147
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-11 20:15:00 UTC
Updated	2022-07-12 17:14:00 UTC
Description	An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragme

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-65	-	All	All	All
Operating System	Arista	C-65 Firmware	-	All	All	All
Hardware	Arista	C-75	-	All	All	All
Operating System	Arista	C-75 Firmware	-	All	All	All
Hardware	Arista	O-90	-	All	All	All
Operating System	Arista	O-90 Firmware	-	All	All	All
Hardware	Arista	W-68	-	All	All	All
Operating System	Arista	W-68 Firmware	-	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.8.9	All	All	All
Hardware	Siemens	Scalance W1700 leee 802.11ac	-	All	All	All
Operating System	Siemens	Scalance W1700 leee 802.11ac Firmware	All	All	All	All
Hardware	Siemens	Scalance W700 leee 802.11n	-	All	All	All
Operating System	Siemens	Scalance W700 leee 802.11n Firmware	All	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](#)

[\[SECURITY\] \[DLA 2689-1\] linux security update](#)

[cert-portal.siemens.com/productcert/pdf/ssa-913875.pdf](#)

[oss-security - various 802.11 security issues - fragattacks.com](#)

[\[SECURITY\] \[DLA 2690-1\] 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)

[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)
591035 Siemens SCALANCE FragAttacks Multiple Vulnerabilities (ICSA-22-104-04) (SSA-913875)
591150 Hitachi ABB Power Grids TropOS Multiple Vulnerabilities (ICSA-21-236-01,9AKK107992A4463)
610373 Google Android Devices October 2021 Security Patch Missing
610383 Google Android November 2021 Security Patch Missing for LGE
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)
690816 Free Berkeley Software Distribution (FreeBSD) Security Update for freebsd-kernel (8d20bd48-a4f3-11ec-90de-1c697aa5a594)
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)

© [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](#)