



# CVE-2020-26146

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

## Summary

<b>CVE</b>	CVE-2020-26146
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-11 20:15:00 UTC
<b>Updated</b>	2021-12-06 13:45:00 UTC
<b>Description</b>	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reass

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Arista</a>	C-100	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-110	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-110 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-120	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-120 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-130	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-130 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-200	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-230	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-230 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-235	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-235 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-250	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-250 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	C-260	-	All	All	All

Operating System	<a href="#">Arista</a>	<a href="#">C-260 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">C-65</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-65 Firmware</a>	-	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">C-75</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">C-75 Firmware</a>	-	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">O-105</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">O-105 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">O-90</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">O-90 Firmware</a>	-	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">W-118</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">W-118 Firmware</a>	All	All	All	All
Hardware	<a href="#">Arista</a>	<a href="#">W-68</a>	-	All	All	All
Operating System	<a href="#">Arista</a>	<a href="#">W-68 Firmware</a>	-	All	All	All
Hardware	<a href="#">Samsung</a>	<a href="#">Galaxy I9305</a>	-	All	All	All
Operating System	<a href="#">Samsung</a>	<a href="#">Galaxy I9305 Firmware</a>	4.4.4	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Scalance W1700 Ieee 802.11ac</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance W1700 Ieee 802.11ac Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Scalance W1750d</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance W1750d Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Scalance W700 Ieee 802.11n</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance W700 Ieee 802.11n Firmware</a>	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

cert-portal.siemens.com/productcert/pdf/ssa-913875.pdf

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

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

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

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

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

390248 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)

43828 HPE ArubaOS Multiple Vulnerabilities (ARUBA-PSA-2021-011)

591035 Siemens SCALANCE FragAttacks Multiple Vulnerabilities (ICSA-22-104-04) (SSA-913875)

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)

610373 Google Android Devices October 2021 Security Patch Missing

610381 Google Android November 2021 Security Patch Missing for Huawei EMUI

610383 Google Android November 2021 Security Patch Missing for LGE

671441 EulerOS Security Update for kernel (EulerOS-SA-2022-1366)

671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

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](#)