



CVE-2020-26145

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

Summary

CVE	CVE-2020-26145
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-11 20:15:00 UTC
Updated	2022-05-13 20:53:00 UTC
Description	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Samsung	Galaxy I9305	-	All	All	All
Operating System	Samsung	Galaxy I9305 Firmware	4.4.4	All	All	All
Hardware	Siemens	6gk5763-1al00-3aa0	-	All	All	All
Operating System	Siemens	6gk5763-1al00-3aa0 Firmware	All	All	All	All
Hardware	Siemens	6gk5763-1al00-3da0	-	All	All	All
Operating System	Siemens	6gk5763-1al00-3da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5763-1al00-7da0	-	All	All	All
Operating System	Siemens	6gk5763-1al00-7da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-3da0	-	All	All	All
Operating System	Siemens	6gk5766-1ge00-3da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-3db0	-	All	All	All
Operating System	Siemens	6gk5766-1ge00-3db0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-7da0	-	All	All	All
Operating System	Siemens	6gk5766-1ge00-7da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-7db0	-	All	All	All
Operating System	Siemens	6gk5766-1ge00-7db0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-7ta0	-	All	All	All

Operating System	Siemens	6gk5766-1ge00-7ta0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1ge00-7tb0	-	All	All	All
Operating System	Siemens	6gk5766-1ge00-7tb0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1je00-3da0	-	All	All	All
Operating System	Siemens	6gk5766-1je00-3da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1je00-7da0	-	All	All	All
Operating System	Siemens	6gk5766-1je00-7da0 Firmware	All	All	All	All
Hardware	Siemens	6gk5766-1je00-7ta0	-	All	All	All
Operating System	Siemens	6gk5766-1je00-7ta0 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
FragAttacks: Security flaws in all Wi-Fi devices	MISC	www.fragattacks.com	
fragattacks/SUMMARY.md at master · vanhoefm/fragattacks · GitHub	MISC	github.com	
cert-portal.siemens.com/productcert/pdf/ssa-913875.pdf	CONFIRM	cert-portal.siemens.com	
oss-security - various 802.11 security issues - fragattacks.com	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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)
159403 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9459)
159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
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)
239816 Red Hat Update for kernel security (RHSA-2021:4356)

239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
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
610381 Google Android November 2021 Security Patch Missing for Huawei EMUI
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)
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](#)