■ Existing CVEs

	CVE ID	Severity	CVSS	CWE	Published	Description	Reference
	CVE-2014-3902	UNKNOWN	5.8	CWE-310	2014-08-15	The CyberAgent Ameba application 3.x and 4.x before 4.5.0 for Andr	http://jvn.jp/en/jp/JVN
	CVE-2014-6820	UNKNOWN	5.4	CWE-310	2014-09-30	The Amebra Ameba (aka jp.honeytrap15.amebra) application 1.0 for Android	http://www.kb.cert.org/vuls/id/
	CVE-2020-27301	HIGH	8.0	CWE-787	2021-06-04	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices)	https://
	CVE-2020-27302	HIGH	8.0	CWE-787	2021-06-04	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices)	https://
	CVE-2022-29859	CRITICAL	9.8	NVD-CWE-noinfo	2022-04-27	component/common/network/dhcp/dhcps.c in ambiot amb1_sdk (aka SDK for Ameba1) before	https://
	CVE-2022-34326	HIGH	7.5	NVD-CWE-noinfo	2022-09-27	In ambiot amb1_sdk (aka SDK for Ameba1) before 2022-06-20 on Realtek RTL8195AM devices	https://
0	CVE-2019-18178	HIGH	7.5	CWE-416	2019-11-04	Real Time Engineers FreeRTOS+FAT 160919a has a use after free. The function FF_Close()	https://sourceforge.net/
0	CVE-2021-43997	HIGH	7.8	NVD-CWE-noinfo	2021-11-17	FreeRTOS versions 10.2.0 through 10.4.5 do not prevent non-kernel code from calling the	https://github.com/FreeRTOS
0	CVE-2021-27504	HIGH	7.4	CWE-190	2023-11-21	Texas Instruments devices running FREERTOS, malloc returns a valid pointer to a small buffer on ext...	https://www.cisa.gov/news-ev
ecification 4.2	CVE-2023-24023	MEDIUM	6.8	NVD-CWE-noinfo	2023-11-28	Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in	https://doi.org/10.
	CVE-2016-4303	CRITICAL	9.8	CWE-120	2016-09-26	The parse_string function in cjson.c in the cJSON library mishandles UTF8/16 strings, which	http://
	CVE-2020-22283	HIGH	7.5	CWE-120	2021-07-22	A buffer overflow vulnerability in the icmp6_send_response_with_addrs_and_netif() function	https://lists.debian.org/
	CVE-2024-7490	CRITICAL	9.8	CWE-20	2024-08-08	Improper Input Validation vulnerability in Microchip Techology Advanced Software Framework	https://www.microchip.com/
2	CVE-2014-3686	UNKNOWN	6.8	CWE-20	2014-10-16	wpa_supplicant and hostapd 0.7.2 through 2.2, when running with certain configurations and	http://advisories.mageia.org/
2	CVE-2019-9233	HIGH	7.5	CWE-125	2019-09-27	In wpa_supplicant_8, there is a possible out of bounds read due to an incorrect bounds check	https://source.android.com/se
2	CVE-2019-9234	HIGH	7.5	CWE-125	2019-09-27	In wpa_supplicant_8, there is a possible out of bounds read due to a missing bounds check	https://source.android.com/se
2	CVE-2019-9243	MEDIUM	5.5	CWE-125	2019-09-27	In wpa_supplicant_8, there is a possible out of bounds read due to a missing bounds check	https://source.android.com/se
2	CVE-2019-9414	MEDIUM	5.9	CWE-20	2019-09-27	In wpa_supplicant, there is a possible man in the middle vulnerability due to an improper input	https://source.android.com/se
2	CVE-2018-16272	CRITICAL	9.8	CWE-269	2020-01-22	The wpa_supplicant system service in Samsung Galaxy Gear series allows an unprivileged pro	https://
2	CVE-2017-18650	HIGH	7.5	CWE-754	2020-04-07	An issue was discovered on Samsung mobile devices with N(7.x) software. The Samsung WifiStat	https://security.samsungmobile
2	CVE-2024-32991	HIGH	7.5	CWE-16	2024-05-14	Permission verification vulnerability in the wpa_supplicant module Impact: Successful exploitation o...	https://consumer.huawei.com/
2	CVE-2024-5290	HIGH	8.8	CWE-427	2024-08-07	An issue was discovered in Ubuntu wpa_supplicant that resulted in loading of arbitrary shared	https://bugs.launchpad.net/
A, WPA2, IEEE 802.11i	CVE-2024-30804	HIGH	7.4	CWE-304	2024-05-17	The IEEE 802.11 standard sometimes enables an adversary to trick a victim into connecting	https://ieeexplore.ieee.org/