■ New CVEs

SDK	CVE ID	Severity	CVSS	CWE	Published	Description
Ameba SDK	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 2022-03-11 mishandles data structures for DHCP packet data.
Ameba SDK	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 before 284241d70308ff2519e40afd7b284ba892c730a3, the timer task and RX task would be locked when there are frequent and continuous Wi-Fi connection (with four-way handshake) failures in Soft AP mode.
cJSON v1.6.0	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 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a non-hex character in a JSON string, which triggers a heap-based buffer overflow.
lwIP 2.0.2	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 of Free Software Foundation lwIP version git head allows attackers to access sensitive information via a crafted ICMPv6 packet.

■ Existing CVEs

SDK	CVE ID	Severity	CVSS	CWE	Published	Description
Ameba SDK	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 Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
Ameba SDK	CVE-2014-6820	UNKNOWN	5.4	CWE-310	2014-09-30	The Amebra Ameba (aka jp.honeytrap15.amebra) application 1.0.0 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
Ameba SDK	CVE-2020-27301	HIGH	8.0	CWE-787	2021-06-04	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "AES_UnWRAP" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.
Ameba SDK	CVE-2020-27302	HIGH	8.0	CWE-787	2021-06-04	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "memcpy" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.
FreeRTOS v10.2.0	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() is defined in ff_file.c. The file handler pxFile is freed by ffconfigFREE, which (by default) is a macro definition of vPortFree(), but it is reused to flush modified file content from the cache to disk by the function FF_FlushCache().

SDK	CVE ID	Severity	CVSS	CWE	Published	Description
FreeRTOS v10.2.0	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 xPortRaisePrivilege internal function to raise privilege. FreeRTOS versions through 10.4.6 do not prevent a third party that has already independently gained the ability to execute injected code to achieve further privilege escalation by branching directly inside a FreeRTOS MPU API wrapper function with a manually crafted stack frame. These issues affect ARMv7-M MPU ports, and ARMv8-M ports with MPU support enabled (i.e. configENABLE_MPU set to 1). These are fixed in V10.5.0 and in V10.4.3-LTS Patch 3.
FreeRTOS v10.2.0	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 extremely large values, which can trigger an integer overflow vulnerability in 'malloc' for FreeRTOS, resulting in code execution.
Bluetooth Core Specification 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 Bluetooth Core Specification 4.2 through 5.4 allow certain man-in-the-middle attacks that force a short key length, and might lead to discovery of the encryption key and live injection, aka BLUFFS.
lwIP 2.0.2	CVE-2024-7490	CRITICAL	9.8	CWE-20	2024-08-08	Improper Input Validation vulnerability in Microchip Techology Advanced Software Framework example DHCP server can cause remote code execution through a buffer overflow. This vulnerability is associated with program files tinydhcpserver.C and program routines lwip_dhcp_find_option. This issue affects Advanced Software Framework: through 3.52.0.2574. ASF is no longer being supported. Apply provided workaround or migrate to an actively maintained framework.
wpa_supplicant 2.2	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 using wpa_cli or hostapd_cli with action scripts, allows remote attackers to execute arbitrary commands via a crafted frame.
wpa_supplicant 2.2	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. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-122529021
wpa_supplicant 2.2	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. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-122465453
wpa_supplicant 2.2	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. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-120905706
wpa_supplicant 2.2	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 improper input validation of the basicConstraints field of intermediary certificates. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-111893041
wpa_supplicant 2.2	CVE-2018-16272	CRITICAL	9.8	CWE-269	2020-01-22	The wpa_supplicant system service in Samsung Galaxy Gear series allows an unprivileged process to fully control the Wi-Fi interface, due to the lack of its D-Bus security policy configurations. This affects Tizen-based firmwares including Samsung Galaxy Gear series before build RE2.

SDK	CVE ID	Severity	CVSS	CWE	Published	Description
wpa_supplicant 2.2	CVE-2017-18650	HIGH	7.5	CWE-754	2020-04-07	An issue was discovered on Samsung mobile devices with N(7.x) software. There is a WifiStateMachine IllegalArgumentException and reboot if a malformed wpa_supplicant.conf is read. The Samsung ID is SVE-2017-9828 (October 2017).
wpa_supplicant 2.2	CVE-2024-32991	HIGH	7.5	CWE-16	2024-05-14	Permission verification vulnerability in the wpa_supplicant module Impact: Successful exploitation of this vulnerability will affect availability.
wpa_supplicant 2.2	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 objects, which allows a local unprivileged attacker to escalate privileges to the user that wpa_supplicant runs as (usually root). Membership in the netdev group or access to the dbus interface of wpa_supplicant allow an unprivileged user to specify an arbitrary path to a module to be loaded by the wpa_supplicant process; other escalation paths might exist.
IEEE 802.1X, WPA, WPA2, RSN, IEEE 802.11i	CVE-2023-52424	HIGH	7.4	CWE-304	2024-05-17	The IEEE 802.11 standard sometimes enables an adversary to trick a victim into connecting to an unintended or untrusted network with Home WEP, Home WPA3 SAE-loop. Enterprise 802.1X/EAP, Mesh AMPE, or FILS, aka an "SSID Confusion" issue. This occurs because the SSID is not always used to derive the pairwise master key or session keys, and because there is not a protected exchange of an SSID during a 4-way handshake.