■ New CVEs

No new CVEs detected.

■ 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.
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.
Ameba SDK	CVE-2025-49604	MEDIUM	5.4	CWE-122	2025-07-09	For Realtek AmebaD devices, a heap-based buffer overflow was discovered in Ameba-AIoT ameba-arduino-d before version 3.1.9 and ameba-rtos-d before commit c2bfd8216a1cbc19ad2ab5f48f372ecea756d67a on 2025/07/03. In the WLAN driver defragment function, lack of validation of the size of fragmented Wi-Fi frames may lead to a heap-based buffer overflow.
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().
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.

SDK	CVE ID	Severity	CVSS	CWE	Published	Description
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.