ESPRESSIF

Security Advisory

Title	Security Advisory on "BadAlloc" Vulnerabilities
Issue date	2021-10-27
Advisory Number	AR2021-005
Serial Number	CVE-2021-3420 CVE-2021-31571 CVE-2021-31572
Version	V1.0

Issue Summary

BadAlloc is a family of vulnerabilities related to integer overflows in heap handling functions in several RTOSes and libraries. The list of vulnerabilities can be found at https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04 .

• Impact

These vulnerabilities occur when the attacker can cause an application to execute some type of memory allocation operation with an attacker-controlled size. This leads to an integer arithmetic overflow when calculating the size of the allocated memory, and subsequently to a heap buffer overflow or heap corruption.

• Vulnerability details

ESP-IDF is affected by the following vulnerabilities in FreeRTOS: CVE-2021-31571, CVE-2021-31572. ESP-IDF is NOT affected by the vulnerability in Newlib: CVE-2021-3420.

ESP-IDF heap management routines include protection against this type of vulnerabilities since v3.1.4 and v3.2 releases. The oldest maintained release at the time of writing is v3.3.x.

CVE-2021-31571 is related to an overflow in xQueueCreate function and affects ESP-IDF v3.x, v4.0.x until v4.0.3, v4.1.x until v4.1.2, v4.2.x until v4.2.2. ESP-IDF v4.3 and later is not affected. Applications are affected if an attacker can cause the application to call xQueueCreate with element size or element count values controlled by the attacker.

CVE-2021-31572 is related to an overflow in xStreamBufferCreate function. It affects only the following pre-release versions: v4.3-beta1, v4.3-beta2, v4.3-beta3. It doesn’t affect any release versions. As in the case with CVE-2021-31571, applications are affected if the attacker can control the arguments of xStreamBufferCreate function call.

Patched versions of ESP-IDF

ESP-IDF Release	Commit ID
Master	639e7ad
release/v4.3	788312a, part of v4.3 release
release/v4.2	fc7bf95, part of v4.2.2 release
release/v4.1	4922973, part of v4.1.2 release
release/v4.0	5ba7202, part of v4.0.3 release
release/v3.3	fa00fd5, not part of any release yet. Will be included in v3.3.6 bugfix release.

Customers using an older version and unable to upgrade can manually apply the following fixes:

- https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/47338393f1f79558f6144213409f09f81d7c4837
- https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/d05b9c123f2bf9090bce386a244fc934ae44db5b
  (applies only to release/v4.3 branch until 788312a; older and newer versions are not affected)

Recommendations for application developers

Even in the absence of these vulnerabilities, an attacker able to control the sizes of memory allocations done by an application can cause denial of service by exhausting the device memory. We recommend sanitizing and validate the ranges of values received from untrusted sources before using these values in the application. For example, if a protocol or file format includes variable-length data prefixed by the length value, the application should check whether the length value is in the expected range before using it, for example, to allocate a buffer for the data.