安全公告

标题	有关 BadAlloc 系列漏洞的安全公告
发布日期	2021-10-27
公告编号	AR2021-005
编号	CVE-2021-3420 CVE-2021-31571 CVE-2021-31572
版本	V1.0

问题小结

多个实时操作系统（RTOS）和 C 标准库的堆处理函数存在整数溢出风险，这些漏洞被统称为 BadAlloc，完整列表见 https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04。

- **影响**

  当攻击者能够控制应用程序，按照攻击者提供的大小进行内存分配时，BadAlloc 漏洞即可能带来风险。具体来说，攻击者可以通过控制内存分配的大小，使应用程序在计算分配内存时出现整数算法溢出，并随后导致堆缓冲区溢出或堆损坏。

- **漏洞详情**

  ESP-IDF 受 FreeRTOS 中以下漏洞的影响：CVE-2021-31571、CVE-2021-31572。ESP-IDF 不受 Newlib 漏洞 CVE-2021-3420 的影响。

  ESP-IDF 从 v3.1.4 和 v3.2 版本起，已在堆管理例程中增加了针对此类漏洞的保护。 本公告发布之时的最早维护版本为 v3.3.x。

  CVE-2021-31571 与 xQueueCreate 函数中的溢出有关，受此影响的 ESP-IDF 版本包括 v3.x、v4.0.x 至 v4.0.3、v4.1.x 至 v4.1.2、v4.2.x 至 v4.2.2。ESP-IDF v4.3 及之后版本不受影响。如果攻击者可以使应用程序调用 xQueueCreate 函数，并使用攻击者控制的元素大小 (element size) 或元素计数值 (element count) 为参数，则应用程序就可能受到影响。

CVE-2021-31572 与 xStreamBufferCreate 函数中的溢出有关，受此影响的 ESP-IDF 版本仅包括以下预发布版本：v4.3-beta1、v4.3-beta2、v4.3-beta3，不包括任何现有已发布版本。与 CVE-2021-31571 的情况类似，如果攻击者可以控制 xStreamBufferCreate 函数调用的参数，应用程序就可能受到影响。

ESP-IDF 修补版本

ESP-IDF 分支	Commit ID
Master	639e7ad
release/v4.3	788312a, 已在 IDF v4.3 中发布
release/v4.2	fc7bf95，已在 IDF v4.2.2 中发布
release/v4.1	4922973，已在 IDF v4.1.2 中发布
release/v4.0	5ba7202，已在 IDF v4.0.3 中发布
release/v3.3	fa00fd5，尚未在任何 v3.3 版本中发布，将会在 IDF v3.3.6 中发布。

使用旧版本且无法升级的客户可以进行手动修复，方法如下：

- https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/47338393f1f79558f6144213409f09f81d7c4837
- https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/d05b9c123f2bf9090bce386a244fc934ae44db5b
  （仅适用于 release/v4.3 分支 788312a Commit 之前的版本；在此之前或之后的版本不受影响）

给应用程序开发者的建议

即使不存在这些漏洞，攻击者只要能够控制应用程序分配内存的大小，即可通过耗尽设备内存，实现拒绝服务攻击。因此，我们建议，应用程序在接受来自不受信任设备的参数时，应首先进行清理和验证。例如，如果协议或文件格式包含以长度值作为前缀的可变长度数据时，则应用程序应在使用这一参数进行操作前，比如为数据分配缓存空间，应首先检查该长度值是否在预期范围内。