安全公告

标题	关于使用 CPA 和 FI 攻击绕过 ESP32-C3 和 ESP32-C6 安全启动及 flash 加密的安全公告
发布日期	2024/01/05
公告编号	AR2023-007
编号	NA
版本	V1.0

问题小结

ESP32-C3 和 ESP32-C6 芯片上发现了一处硬件漏洞，使用侧信道攻击可以绕过基于 XTS-AES 算法的 flash 加密功能。

此攻击利用相关功耗分析 (CPA)、故障注入 (FI) 和缓冲区溢出漏洞，获得加密 flash 第一个块的控制权。攻击者控制 flash 的第一个块后，向其植入自定义的 shellcode 代码。之后芯片启动时，按照启动流程 shellcode 会加载到内部存储器中。在安全启动机制识别到加载的代码被篡改、中止启动前，CPU 已被诱骗跳转并执行 shellcode。如此一来，攻击者便可通过精心编写 shellcode 获取设备中的机密信息。

- **什么是侧信道攻击 (SCA)？**

  侧信道攻击利用系统意外泄露的信息来获取机密值，通常获取的是加密密钥。侧信道攻击有多种形式，包括时序变化或设备功耗。

  此公告中针对 ESP32-C3 和 ESP32-C6 的侧信道攻击采用相关功耗分析 (CPA) 的形式。

- **什么是故障注入？**

故障注入攻击指在系统中人为注入错误或故障（例如电压或时钟），评估系统的恢复机制和容错能力。攻击者通过注入的故障操控系统行为，旨在找到系统的弱点，利用潜在的安全漏洞。

此公告中针对 ESP32-C3 和 ESP32-C6 故障注入攻击基于电压故障注入。这是一种侵入性攻击，需要一定水平的专业知识、精确性和资源才能实施，对许多攻击者来说不太可行。

- **影响分析**

1. 受到攻击的芯片用 XTS-AES 加密模式进行 flash 加密，每个 flash 块有单独的加密密钥。攻击者使用 CPA 技术，可以获取第一个 flash 块的加密密钥，之后使用该密钥获取设备的机密信息。

2. 使用 CPA 攻击恢复密钥需要大量的功耗追踪数据（约 600,000），并且要花费 5 天的时间。此外，CPA 攻击无法恢复 tweak 密钥（可调整密钥），只能恢复每个块的 tweak 值，也就是说每次攻击能破解的数据仅 128 字节。而且，要破解 XTS-AES 加密模式，tweak 值和加密密钥缺一不可。这令实施攻击变的更加复杂。

3. 就所需的精力和时间来看，使用第 2 点提到的技术解密整个加密 flash 是不切实际的。

4. 此攻击还需要绕过安全启动，并利用故障注入（精心设计的电压毛刺）让 ROM 代码缓冲区溢出，从而加载和执行内部存储器中的 shellcode。

5. 获取加密密钥的过程复杂、耗费时间长，使得攻击者能在设备上加载、执行的 shellcode 大小受限，给攻击者造成又一重障碍，起到了威慑作用。由于每个设备使用的 flash 加密密钥唯一，此攻击无法扩展到同类别设备。

缓解措施

目前针对此问题尚无软件和硬件修复方案。后续产品将采取硬件措施解决这些问题。以下是可以缓解问题的建议。

- **硬件级措施**

SCA 攻击：使用防篡改机制保护设备免于物理访问，该机制一旦破解便会被检测到，可以有效避免故障注入攻击。设备在检测到篡改时会执行预定操作，如复位设备、清除设备上的机密信息。

- **应用级措施**

  加密密钥如果与其他设备或制造批次相同，一定不能长期使用。

  实施此类攻击需要大量精力、高超技能以及昂贵复杂的实验室设备。如果每个设备都配有与设备标识关联的唯一密钥，攻击者就无法将攻击扩展到同类别设备，不值得实施攻击。此外，我们建议芯片用户同时开启 flash 加密和安全启动功能，最大限度减少攻击者重写固件的风险。

  乐鑫的几款系统级封装 (SiP) 产品（如 ESP32-PICO-V3） flash 管脚未引出，可以更好地防范此类攻击。管脚未引出意味着不能使用外部 flash 模拟器，且无法监测 flash 管脚，无法如本公告所述攻击 flash 加密功能。

其他乐鑫产品

理论上，CPA 攻击可能适用于使用 XTS-AES 的所有芯片，包括 ESP32-C2、ESP32-C3、ESP32-S2、ESP32-S3、ESP32-C6、ESP32-H2、ESP32-P4 和 ESP32-C5。而在 ESP32-C5 的 XTS-AES 中，新增了伪轮机制以抵抗旁路攻击，实施 CPA 攻击的难度将大幅度上升。但是，能否成功实施全套攻击还取决于故障注入 (FI) 的可行性，这一点则与每个芯片系列的 ROM 紧密相关。在后续系列芯片（ESP32-H2、ESP32-P4、ESP32-C5 等）中，硬件自带的 glitch 检测电路可以检测出该攻击中所使用的 glitch，一旦出现这种 glitch，芯片会自动复位。

ESP32（包括芯片版本 v3.0 和 v3.1）不使用 XTS-AES 机制，因此本公告未讨论 CPA 和 FI 联合攻击对 ESP32 的影响。

致谢

感谢优秀硬件和固件工程师 **Kévin Courdesses** 报告此漏洞，并协助我们跟进本次披露。