安全公告

标题	ESP32-H2 ECDSA 外设的时间分析攻击安全漏洞
发布日期	2024/11/26
公告编号	AR2024-007
编号	NA
版本	V1.0

问题小结

ESP32-H2 芯片 v1.2 之前的版本存在硬件漏洞，由于 ECDSA 外设未以恒定时间运行，导致其易受时间分析攻击。然而，启用安全启动可以显著降低此类攻击的概率，因为这些攻击需要包含受控数据模式的大量样本。

什么是格攻击(Lattice Attack)？

格攻击只需找出多个签名，了解它们参数 k 的少数几个比特位（k 为 ECDSA 算法中的随机数），就能危及整个私钥的安全。

本文所述对 ESP32-H2 的攻击生成了许多签名，找出其中对应 k 的最高有效位大概率包含多个零的签名。其实现方式为生成大量签名，并筛选出生成时间低于特定阈值的签名。在以此方式筛选出待攻击的签名后，应用 BKZ 格基规约算法来获取 ECDSA 私钥。

问题详情

此攻击利用 ECDSA 外设在执行 ECC 点乘时不同乘数的计算时间差异，使用格攻击算法来获取 ECDSA 私钥。此外，当前 eFuse 配置中无法区分 ECDSA P192 和 ECDSA P256 密钥的用途，从而减少了进行时间分析所需的工作量。

影响分析

1. 为了实施攻击，攻击者需要计算硬件生成 ECDSA 签名的时间。这可以通过几种方法完成，每种方法都有显著的局限性：

- 攻击者远程获取 ECDSA 签名的时间，这种方法要求通信延迟非常稳定且没有其他时间上的不确定性。

- 攻击者使用功耗分析计算签名时间，这种方法需要测量设备以及对芯片的直接接触。

- 攻击者直接操作 ECDSA 外设计算签名时间，这种方法需要绕过多个安全机制，例如安全启动和 flash 加密，成本高昂。

2. 通过分步攻击可以降低攻击难度，即首先猜测使用 ECDSA P-192 曲线运算的 192 位，然后暴力破解 ECDSA P-256 私钥中剩余的 64 位。

3. 实施攻击需要大量样本，并且需要相当的精力和时间。计算 ECDSA 签名时间的准确性直接影响到成功率。攻击目标是生成时间快于阈值的签名，然而即使准确度轻微下降也会显著增加攻击时间。

影响产品系列

基于时间分析的格攻击理论上适用于所有包含 ECC 加速器且支持硬件加速 ECDSA 签名的 SoC，即 ESP32-H2（< v1.2）。我们已经实现软件修复，并在 ESP32-H2 v1.2 中引入了硬件对策。请注意，硬件对策已在 ESP32-C5 和 ESP32-C61 中实施，并将纳入所有未来的 SoC，以应对这一安全漏洞。

影响 SoC

SoC	**影响芯片版本**	**修复芯片版本**
ESP32-H2	< v1.2	v1.2 及之后

注：了解如何判断 ESP32-H2 芯片版本，请参考芯片版本标识。

应对方法

软件对策

针对目前受影响的 ESP32-H2 芯片版本（< v1.2），软件对策为在 ECDSA 驱动中随机化功耗特征,使其成为恒定时间。请注意，必须启用安全启动，软件对策才能完全生效。对于受影响的 ESP32-H2 芯片版本，以下版本的 SDK 默认启用这一软件对策。

ESP-IDF 修复版本

ESP-IDF 分支	修复 Commit IDs	ESP-IDF 修复版本
master	5bfa1fb	NA
release/v5.3	4f29e3f	预计在 5.3.2 中修复
release/v5.2	2b2869a	预计在 5.2.5 中修复
release/v5.1	8b2abcc	5.1.5

硬件对策

我们在 ECDSA 和 ECC 外设硬件中引入了一种安全模式，使 ECC 运算以恒定的时间和功耗进行。这种方式可以防止在运行时或从功耗上泄漏 k 的位值。此外，我们增加了新的 eFuse 配置位，限制 ECDSA 硬件仅使用固定的 ECC 曲线进行签名/验证。请注意，ESP32-H2 v1.2 芯片版本已经包含相关修复。

其他乐鑫产品

此问题仅影响支持 ECDSA 外设的芯片，其中 ESP32-C5 和 ESP32-C61 已经实施硬件对策。其他芯片不支持 ECDSA。

致谢

感谢优秀的硬件和软件工程师 Emil Lenngren 报告此漏洞，并协助我们跟进本次披露。