安全公告

标题	有关 ESP32 芯片版本 v3.0 硬件 AES 内核与固件加密漏洞的安全公告
发布日期	2022/11/18
公告编号	AR2022-003
编号	NA
版本	V2.0

问题小结

Ledger (Donjon) 的安全研究人员公布了 ESP32 芯片版本 v3.0 芯片的两处硬件漏洞。

据称，这两处漏洞分别位于 ESP32 芯片版本 v3.0 芯片的硬件 AES 内核和 flash 加密功能。这两处漏洞可通过侧通道攻击手段或体偏置注入攻击手段产生。

- **侧通道攻击**

  漏洞表明，对芯片设备具有物理访问权限的攻击者可以发起侧通道攻击 (Side Channel Attack, SCA)，进而从芯片的硬件 AES 内核获取加密密钥或者获取芯片 eFuse 中存储的 flash 加密密钥。

  为了成功实施针对芯片的 SCA 攻击：首先，攻击者需要追踪分析数以万计的功耗数据，并通过适当的信噪比计算，来识别 AES 运算的时间局部性。其次，他们需要在同一位置以汉明权重为泄漏模型，发起 CPA 攻击。最终，找出 AES 运算中使用的实际密钥。

  - **侧通道攻击 (SCA) 是什么?**

    电子设备在运行时，可能会泄漏与其内部运行相关的信息，比如设备功耗或产生的电磁辐射变化等。

    当设备在处理一些安全敏感数据（例如加密密钥）时，这些泄漏的信息可能会被用来从设备中提取密钥，从而导致设备安全性受损。SCA 是一种非侵入性攻击，攻

击者在执行 SCA 攻击过程中，需要拆开设备以获取设备的瞬时功耗轨迹，但不需要拆开芯片封装。这对设备来说是一个真正的威胁，但攻击者需要一定技巧才能成功发起攻击。

一些常见的 SCA 技术包括：

- ✓ 简单功率分析（SPA）
- ✓ 差分功率分析（DPA）
- ✓ 相关功率分析（CPA）

- **体偏置注入攻击**

针对硬件 AES 漏洞，对芯片设备具有物理访问权限的攻击者还可以发起体偏置注入攻击 BBI 攻击 (Body Biasing Injection, BBI)，进而从芯片的硬件 AES 内核获取加密密钥。

为了成功实施针对芯片的 BBI 攻击：首先，攻击者需要确定 AES 内核在芯片 DIE 上的精确位置。其次，他们需要追踪分析大量功耗数据，通过计算信噪比来识别 AES 运算的时间局部性。其次，他们需要在同一位置附近发起相当多次的 BBI 攻击。最终，找出 AES 运算中使用的实际密钥。

- **体偏置注入攻击（BBI）是什么？**

BBI 攻击于 2012 年被首次提出，攻击方式很是新颖，正因为如此，BBI 对设备来说是一个真正的威胁，但攻击者需要一定技巧才能成功发起攻击，比如它要求打开封装，从芯片背板进行攻击。这种攻击手段的一些依据是：

- ✓ 对芯片衬底上的某个点施加一个幅度适当的电压脉冲，会导致芯片电路中出现某些逻辑从 0 到 1 的翻转（或 1 到 0 的翻转）。
- ✓ AES 运算本质上是一个迭代运算，其算法特征决定了在某次迭代前的单 byte 错误会在本次迭代运算完成后扩散至 4 个 byte 错误，且这 4 个错误 byte 的位置和单 byte 错误的位置存在相关性，这种相关性会反向暴露出单 byte 错误的位置。
- ✓ AES 运算中存在基于伽罗华域上的非线性运算，密文中的 4 个 byte 错误之间携带有秘钥特征，而这允许攻击者在纯数学层面上反向统计推导获取到秘钥。

- **影响分析**

1) 硬件 AES-256 内核漏洞

SCA 和 BBI 攻击将危及 AES 密钥长期存在或永久保存在设备中的系统。

在 AES 密钥寿命较短的用例中，例如 TLS 会话密钥，这两种攻击不会产生直接影响。

2) 硬件 Flash 加密漏洞

在获取 flash 加密密钥后，SCA 攻击者可能从设备加密 flash 中获取任何现存的机密信息。

如果同时配合其他攻击，SCA 攻击者可将 flash 中的加密内容替换为自己精心设计的内容，并接管设备。

但是，如果已遵循建议做法，即每部设备 eFuse 中保存的 flash 加密密钥均是唯一的，则 SCA 攻击仅限于特定设备，很难形成规模化攻击。

应对方法

目前，针对现有芯片尚无方法从硬件方面解决此问题，未来的新产品将在芯片中加入硬件对策，以解决这些问题。

以下是应对这两处漏洞的一些建议。

- **软件对策**

可以使用伪 AES 操作屏蔽 AES 内核中的真实 AES 操作。此举可以增加攻击者在收集到的功率跟踪中识别真实 AES 操作的难度。值得指出的是，这种对策会影响 AES 的运行性能。

我们将评估软件对策及其对性能的影响。如通过评估，我们将在未来的 ESP-IDF 版本中增加额外的项目 menuconfig 配置选项，允许用户自行选择是否使用伪 AES 操作屏蔽真实 AES 操作。

- **硬件对策**

针对 SCA 技术：可通过采用硬件防篡改机制，保护设备免受非法物理访问。这种硬件防篡改机制一旦受到破坏，设备应按照预定动作进行响应，例如重置设备、清除设备上的机密信息等。

针对 BBI 技术：目前硬件层面上并没有很好的抵御 BBI 攻击的方法。

- 应用对策

  乐鑫芯片使用者应不惜一切代价避免同类设备或同生产批次设备共用同一个长期加密密钥。

  在设备上成功实施这些攻击并不容易，需要付出巨大的努力、具备很多专业技能且必须使用昂贵而复杂的实验室设备。因此，如果每部设备均采用唯一的密钥，则攻击者将无法实施针对同一类设备的规模化攻击，从而降低这种攻击的吸引力。此外，我们建议芯片使用者同时启用 Flash 加密和 Secure boot，可以尽量避免攻击者篡改固件的风险。

  目前，乐鑫多款 SiP 封装芯片（比如 ESP32-PICO-V3）的 flash 管脚并未从内部引出，可以防止攻击者使用任何外部 flash 仿真器或监控 flash 加密等相关功能所使用的 flash 管脚，因此可以更好地抵御此类攻击。

涉及乐鑫产品

本公告中报告的 SCA 漏洞和 BBI 漏洞可能适用于的乐鑫 SoC，包括 ESP32 、ESP32-S2、ESP32-C3 和 ESP32-S3。我们将在未来的芯片中加入硬件对策，以解决这些漏洞。

ESP32-S2、ESP32-S3、ESP32-C3、ESP32-C2 的硬件 flash 加密功能已经将加密算法升级为更复杂的 XTS-AES 算法，借此增加实施 SCA 攻击的难度和成本，从而降低安全风险。

致谢

我们感谢 Donjon Ledger 的 Karim M.Abdellatif、Olivier Hériveaux 和 Adrian Thillard 报告了这两处漏洞，并协助我们跟进了本次披露。

修订历史

日期	版本	发布说明
2022/11/18	V2.0	新增体偏置注入攻击（BBI）技术及其影响和对策。
2022/05/23	V1.1	更正章节 *侧通道攻击* 中 SPA 的全称。
2022/05/18	V1.0	首次发布。