安全公告

标题	有关利用 EMFI 绕过安全启动和 flash 加密的安全公告
发布日期	2023/07/11
公告编号	AR2022-005
编号	CVE-2023-35818
版本	V1.0

问题小结

Raelize 和 **Technology Innovation Institute (TII)** 的安全研究人员发现了一处漏洞，该漏洞涉及使用电磁故障注入（EMFI）技术攻击 ESP32 芯片版本 v3.0。通过 EMFI 技术，能够以可控的方式改变 ESP32 的执行流程，使其直接跳转至由 ROM 代码实现的 UART 下载模式。当释放模式配置启用安全启动 (V2) 和 flash 加密功能，并永久禁用 UART 下载模式时，可能发生上述情况。

- **EMFI 是什么？**

  EMFI 是一种侧通道攻击技术，可以通过电磁脉冲改变嵌入式设备的行为。该技术使用主动探测器在芯片表面施加极强的电磁场，导致存储器表面出现故障，从而改变存储器中保存的数值。某些情况下，若移除芯片的金属屏蔽层，该技术对芯片表面的探测能力将有所提升。

  此类攻击的难点在于，为达成攻击目标，攻击者需要通过大量实验来确定芯片表面的空间位置。如果成功使用 EMFI 改变了存储器中的内容，那么攻击者便得以控制设备的执行流程。

- **问题详情**

  攻击者如果具备 ESP32 设备和精密实验器材的物理访问权限，便可确定芯片上的空间位置以及故障延迟和功率等攻击参数。借助由此产生的攻击向量，攻击者能够按预期改变运行时的 CPU 的 PC 值 (Program Counter，程序计数器) 。

  一旦攻击者利用 EMFI 成功控制 PC，就可以使 PC 跳转至 UART 下载模式等可以利用 ROM 代码的位置，从而绕过安全启动。

  操纵 PC 值的前提是 ESP32 flash 中一定有可执行的程序。借助安全启动和 flash 加密等安全功能，研究人员谨慎地使用 ROM 串行日志中的调试信息，通过不断尝试，最终找到了将任意地址注入 CPU PC 的方法以复现 EMFI 攻击。

- **影响分析**

  攻击者对 ESP32 进行 EMFI 攻击，能够不受安全启动和 flash 加密状态的限制，在 CPU 上下文级别影响 PC 值。此外，在 ESP32 中，ROM 程序中的 UART 下载模式入口没有经过强化以抵御故障注入攻击。

  利用这两个漏洞，攻击者可以绕过安全功能，迫使 CPU 进入 ROM UART 下载模式，并通过 UART 信道与芯片进行通讯。这样一来，攻击者能够加载和执行任意存根代码（仅限内部存储器），或者从 flash 中读取解密内容。

  这是一种半入侵式攻击，需要较高的技巧和精度来定位芯片上特定的空间和时间位置。该攻击方式的成功率较低，这可以对攻击者起到一定的震慑作用。

应对方法

目前尚无立竿见影的应对方法，以下建议可供参考。

攻击者需要花费大量时间、具备较高技能且拥有昂贵而精密的实验器材，才能成功攻击设备。若能为每个设备都配备与其身份关联的唯一密钥，那么攻击者则无法在攻破单个设备后，将攻击成果扩展至所有芯片设备，从而降低发起攻击的可能性。

乐鑫多款 SiP 封装芯片（如 ESP32-PICO-V3 和 ESP32-PICO-V3-02）的 flash 管脚位于内部而未引出。SiP 有助于抵御此类攻击，因为攻击者需要使用外部 flash 编程器篡改其中的内容。

其他乐鑫产品

ESP32 芯片版本 v3.0 和 v3.1 容易受到此类攻击。请注意，ESP32 之前的芯片版本无法永久禁用 UART 下载模式，故也容易受到此类攻击，这里不展开描述。

ESP32-S2、ESP32-C3、ESP32-S3 和未来所有芯片的 ROM 代码中，均包含阻止类似故障注入攻击的防护措施。

致谢

感谢 **Raelize** 的 **Cristofaro Mune** 和 **Niek Timmers** 以及 **Technology Innovation Institute (TII)** 的 **Jeroen Delvaux** 和 **Mario Romero** 报告此漏洞，并协助我们跟进本次披露。