乐鑫安全事件响应流程

版本 1.0
乐鑫信息科技

目录

1. 简介

乐鑫致力于确保产品和软件解决方案的安全性。我们认识到安全事件是一种持续存在的威胁，因此，我们高度重视及时、高效地响应安全事件并提出缓解措施。

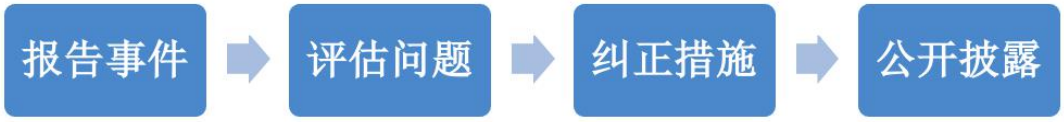
本文档介绍了乐鑫硬件产品和软件解决方案中可能出现的安全事件的处理流程。我们会定期审阅和更新该流程，确保流程的有效性，向行业最佳实践看齐。

2. 响应流程

流程开始的标志为问题的发现，问题可能来源于第三方项目披露、研究人员、漏洞报告（包括乐鑫漏洞赏金计划，BBP）、客户报告、内部发现等。

流程结束的标志为所有相关修复措施和安全公告（如适用）的发布。安全公告发布在乐鑫官网 > 公告页面 > **安全**类别，涉及硬件和软件方面。ESP-IDF 软件组件相关的公告发布在 ESP-IDF GitHub 仓库 > Security 页面。

处理流程：



2.1. 报告事件

安全事件可以通过多种方式报告，报告的提出者可以是乐鑫内部员工，也可以是外部客户、研究人员或其他相关方。报告人可以通过以下方式提交安全漏洞：

- 硬件问题表格和软件 BUG 表格
- 乐鑫漏洞赏金计划（通过 bugbounty@espressif.com 报告的乐鑫软件解决方案中的安全问题可能入选漏洞赏金计划）

注意：考虑到安全漏洞报告中可能存在敏感信息，乐鑫强烈建议所有报告使用乐鑫的 PGP/GPG 密钥以加密格式提交。

- 指纹：A855 92F9 A412 44C1 13F9 0F0F 01C3 E225 A0FE D438
- 公共密钥文件 (ZIP, 4 KB)

请使用以下免费软件来读写 PGP/GPG 加密消息：

- Gpg4win
- GnuPG

报告潜在的安全漏洞时，请提供尽可能多的必要信息，以便帮助我们正确地评估该漏洞。需要报告的内容包括但不限于：

- 清晰简洁的问题标题，指出受到影响的乐鑫产品，包括产品名称或型号。
- 问题描述，包括测试期间使用的软件版本、硬件版本、使用的工具和其他环境因素、期待的测试结果和实际的测试结果，以及问题可能造成的安全影响。
- 复现问题的完整步骤，详细的测试代码（编译后可运行）和调试日志，以及其他任何可能相关的信息。

如果缺乏足够的信息，评估过程可能会更长。

2.2. 评估问题

- 内部评估报告是否提供了所有的必要信息，分配优先级，确定追踪方式。
- 从技术角度分析、验证问题，确定对产品的影响。评估安全风险并对问题进行分类。
- 预估时间：4 周。

2.3. 纠正措施

- 对于验证后确实存在的漏洞，提出修复或缓解措施。
- 向报告提交者和其他相关人员传达响应措施：
  - 修复措施的时间表和修复的版本。请报告者验证补丁（如适用）。
  - 预计发布安全公告的时间表（如适用）。
  - 分析是否需要为该问题注册 CVE。
  - 确定是否符合漏洞赏金计划的要求以及奖励级别（如适用）。
- 部署修复和缓解措施。
- 准备和审阅安全事件公告并保留 CVE 编号（如适用）。
- 预估时间：从开始算起 8 周，约 2 个月

2.4. 公开披露

在约定的披露日期：

- 发布公告，包括调查结果、影响、缓解措施、以及产品路线图中的安全增强计划。公布 CVE 编号。
- 确保其他的修复措施迅速部署到软件堆栈中，如 ESP-IDF。
- 对于符合漏洞赏金计划的安全问题，支付合理的赏金。
- 如有必要，通知受到影响的乐鑫客户。
- 时间估计：从开始算起 12 周，约 3 个月

注：上述的预计时间是一般情况下的典型时间表，实际时间可能会因问题的严重性和复杂性而有所不同。

3. 披露政策

乐鑫高度重视安全研究人员的贡献和他们在增强我们产品安全方面的重要作用。为确保安全事件响应的有效性，我们建议事件报告人遵循协调漏洞披露流程，即向我们报告漏洞，并允许一定时间进行调查和修复，然后再公开披露任何信息。此外，我们还建议事件报告人在未经乐鑫事先授权的情况下不要披露任何未解决或未发布的漏洞。

在协调漏洞披露过程中，乐鑫也会严格保守机密信息。 乐鑫和事件报告人之间共享的任何信息都将保密，并且仅用于处理报告的漏洞的目的。

乐鑫衷心感谢所有为保障我们产品和用户的安全做出贡献的人。

www.espressif.com

免责声明和版权公告

本文档中的信息，包括供参考的 URL 地址，如有变更，恕不另行通知。

本文档可能引用了第三方的信息，所有引用的信息均为“按现状”提供，乐鑫不对信息的准确性、真实性做任何保证。

乐鑫不对本文档的内容做任何保证，包括内容的适销性、是否适用于特定用途，也不提供任何其他乐鑫提案、规格书或样品在他处提到的任何保证。

乐鑫不对本文档是否侵犯第三方权利做任何保证，也不对使用本文档内信息导致的任何侵犯知识产权的行为负责。本文档在此未以禁止反言或其他方式授予任何知识产权许可，不管是明示许可还是暗示许可。

Wi-Fi 联盟成员标志归 Wi-Fi 联盟所有。蓝牙标志是 Bluetooth SIG 的注册商标。

文档中提到的所有商标名称、商标和注册商标均属其各自所有者的财产，特此声明。