# 网络安全漏洞管理原则

Moxa 致力于打造稳固的产品[i]网络漏洞响应程序，向客户提供可靠的操作指南和解决方案，尽可能减少客户的网络安全风险。为此，Moxa 设立产品网络安全响应小组 (PSIRT)，负责应对产品网络安全事件和可能出现的产品漏洞事宜。Moxa 始终以广为接受和使用的国际行业标准[ii]为准绳，推行网络安全实践，不断优化网络安全漏洞处理程序与响应措施，以积极态度支持工业网络安全，成为值得客户信赖的合作伙伴。

## 产品网络安全漏洞管理程序

Moxa 产品网络安全漏洞管理程序分为五个阶段，每一阶段都有具体流程和操作要求。Moxa 严格遵循以下网络安全做法。


图 1：网络安全漏洞管理程序

- 首次回应：PSIRT 收到关于 Moxa 产品漏洞的外部报告后，将在两个工作日内联系报告人，作出首次回应。
- 评估分类：PSIRT 将对报告所涉产品网络安全漏洞进行分析与分类，以初步确认该漏洞对 Moxa 产品的影响程度。此阶段结束后，Moxa 会向报告人提供初步评估结果。
- 调查研究：PSIRT 将与产品开发团队协作，找出漏洞的根本原因，评估漏洞对 Moxa 产品的影响程度与范围，进而提出减轻风险、修复漏洞的解决方案。在此阶段，PSIRT 会与报告人保持积极沟通。
- 漏洞修复：PSIRT 将与产品开发团队协作，开发软件/固件修复补丁，或确定风险缓解措施。同时，PSIRT 将持续关注相关漏洞的信息以正确评估漏洞的严重性。如果漏洞风险等级较高，且补丁开发所需的时间较长，Moxa 会在最终修复方案完成前，先向客户提供应急缓解措施。
- 信息公开：PSIRT 将在 Moxa 网站的“安全公告”页面发布网络安全漏洞的处置结果。内容包括：漏洞说明、可能受影响的产品和版本、缓解措施、修复计划等。

Moxa PSIRT 与研发团队利用通用漏洞评分系统 (CVSS) 及 Moxa 风险漏洞管理模型，根据安全情境、漏洞被利用的可能性及其影响等因素，评估该网络安全漏洞的潜在风险，并据此确定解决问题的时间表。

在确认该漏洞对 Moxa 产品的影响后，Moxa 将立即搭建专用的测试环境，评估漏洞的严重性，必要时将与漏洞报告人进一步沟通。在确定漏洞的根本原因及其对 Moxa 产品的影响程度后，Moxa 会进行修复分析，并提供解决方案或风险缓解措施。

关于产品网络安全公告的更新与发布，请参阅 Moxa 官网“安全公告”页面。Moxa 用户可以通过 RSS 阅读器订阅 Moxa 安全公告。如需获取特定产品的最新安全信息，可以注册 Moxa 账号并点击“关注更新”选项。

## 产品网络安全漏洞联络窗口

如果您在任何 Moxa 产品中发现可疑漏洞，请立即向 Moxa 报告。对 Moxa 而言，及时发现网络安全漏洞是降低产品安全风险的关键。您可以通过邮件告知 PSIRT 产品网络安全漏洞的相关信息。请使用 Moxa PSIRT 的 PGP 密钥为您的消息和文件加密。

报告产品网络安全漏洞时，为了提高风险评估和修复措施开发的速度，请您提供以下信息：

1. 产品名称与型号
2. 软件/固件版本
3. 重现事件经过所需的设备及软件
4. 重现事件经过的步骤（如果可以，请附上图片或程序代码）
5. 概念验证利用代码
6. 简要描述攻击者可以如何利用该漏洞
7. 攻击过程的封包侧录（可使用 Wireshark 等工具）
8. 其他您认为有价值的信息

- PSIRT 电子邮箱：PSIRT@moxa.com
- 下载 Moxa PGP 密钥

**免责声明**

网络安全漏洞管理原则的具体内容可能会视个案情况而有所变更。我们不保证对任何特定问题做出回应。若使用本文件包含的信息或本文件中链接的内容，需由您自行承担风险。Moxa 保

留随时修改本原则中任何内容的权利，恕不另行通知。如有任何修改，修改后的文件将发布于 Moxa 官方网站：www.moxa.com.cn。

---

[i] “产品”是指市场上所有 Moxa 标准产品。非标准产品，如用户定制的产品，则依照相关合约内容进行维护与响应。

[ii] Moxa 参照多项标准，包括：

- 应急响应与安全组论坛 (FIRST) 制定的通用漏洞评分系统
- FIRST 制定的 PSIRT 服务标准 1.1 版本
- ISO/IEC 29147:2018 漏洞信息公开标准