产品安全公告

2023 年 1 月 13 日

InHand-PSA-2023-01

CVE-2023-22597,CVE-2023-22598, CVE-2023-22599,

CVE-2023-22600, CVE-2023-22601

概述

映翰通网络针对 IR302 工业路由器存在的已知安全漏洞进行声明并提供安全漏洞的修复措施。该产品存在一些已知的安全漏洞，成功利用这些漏洞可以实现消息排队遥测传输（MQTT）命令注入，未经授权披露敏感设备信息，以及远程代码执行。如果将这些漏洞组合成攻击链使用，那么这可能导致未经授权的用户破坏每一个云管理的 InHand Networks 设备。

映翰通网络建议客户将固件版本升级至 InRouter3XX-V3.5.56 及以上版本，以修复当前已知的安全漏洞。

影响

- CVE-2023-22597:

  CVSSv3 Score 6.5

  受影响的产品默认使用不安全的通道与云平台通信。导致敏感信息泄露和其他的攻击利用。

- CVE-2023-22598:

  CVSSv3 Score 7.2

  受影响的产品容易受到系统命令注入攻击。

- CVE-2023-22599:

  CVSSv3 Score 7.0

  受影响的产品响应来自云平台的 HTTP/HTTPS 请求时所发送的 MQTT 凭据使用了较容易计算的加密算法。

- CVE-2023-22600:

  CVSSv3 Score10.0

  受影响的产品允许未经身份验证的设备订阅 MQTT 主题。这包括发送 GET/SET 配置命令、重启命令和推送固件更新。

- CVE-2023-22601:

  CVSSv3 Score 5.3

  受影响的产品没有正确随机化 MQTT ClientID 参数。未经授权的用户可以计算这个参数并利用它来收集同一云平台上管理的其他 InHand 设备的额外信息。

受影响的产品和版本

- 工业路由器 IR302，固件版本 InRouter3XX-V3.5.56 之前的版本。

解决措施

- 下载并升级至 InRouter3XX-V3.5.56 及以上版本。

致谢

OTORIO 的 Roni Gavrilov 师傅。

映翰通产品安全公告

首次发布日期

2023 年 1 月 13 日

资源

安全解决方案页面：

https://www.inhand.com.cn/product-security-advisories.html

https://www.cisa.gov/uscert/ics/advisories

CVE-2023-22597

CVE-2023-22598

CVE-2023-22599

CVE-2023-22600

CVE-2023-22601