产品安全公告

2023 年 3 月 14 日

InHand-PSA-2023-03

FG-VD-22-101, FG-VD-22-106, FG-VD-22-107,

FG-VD-22-108,FG-VD-22-109

概述

映翰通网络针对 InRouter615-S 工业路由器存在的已知安全漏洞进行声明并提供相应的修复措施。该产品的特定固件版本存在一些已知的安全漏洞，攻击者可利用这些漏洞对受影响的设备发起拒绝服务攻击、获取账号密码信息、暴力破解密码等操作。

映翰通网络建议客户将受到影响的设备固件版本升级至 InRouter6XX-S-V2.3.0.r5550，以修复当前已知的安全漏洞。

影响

- FG-VD-22-101:

  CVSSv3 评分：6.5

  受影响产品的 apply.cgi 没有过滤输入参数，非格式化输入可能造成接口拒绝服务。

- FG-VD-22-106:

  CVSSv3 评分：6.5

受影响产品没有对密码显示进行加密处理，存在密码信息泄露的风险。

- FG-VD-22-107:

  CVSSv3 评分：5.3

  受影响产品的 SSH 没有做登录限制，攻击者可使用暴力破解进行攻击。

- FG-VD-22-108:

  CVSSv3 评分：8.8

  受影响产品的 OpenVPN 配置页面存在 XSS 漏洞。

- FG-VD-22-109:

  CVSSv3 评分：8.8

  受影响产品的 IPSec Tunnels 配置页面存在 XSS 漏洞。

受影响的产品和版本

- 工业路由器 InRouter615-S，固件版本 InRouter6XX-S-V2.3.0.r5542 以及之前版本。

解决措施

- 下载并升级至 InRouter6XX-S-V2.3.0.r5550。

致谢

Fortinet's FortiGuard Labs 实验室的 YangZhouyuan。

首次发布日期

2023 年 3 月 14 日

资源

安全解决方案页面：https://www.inhand.com.cn/product-security-advisories.html

https://fortiguard.com/zeroday