产品安全公告

2021 年 11 月 1 日

InHand-PSA-2021-01

CVE-2021-38472, CVE-2021-38486, CVE-2021-38480,
CVE-2021-38464, CVE-2021-38474, CVE-2021-38484,
CVE-2021-38466, CVE-2021-38470, CVE-2021-38478,
CVE-2021-38482, CVE-2021-38468, CVE-2021-38476,
CVE-2021-38462

ICSA-21-280-01

概述

映翰通网络针对 IR615-S 路由器存在的已知安全漏洞进行声明并提供安全漏洞修复措施。该产品的 web GUI 配置存在校验不足、授权校验不足、弱密码策略、跨站点脚本以及加密强度不足等产品安全漏洞。

经风险评估，攻击者可能会利用这些漏洞进行尝试登录设备或者利用弱密码暴力破解设备，映翰通网络建议客户应将固件升级到版本 InRouter6XX-S-V2.3.0.r5484，以修复当前暴露的安全漏洞问题。

影响

- IR615-S 的管理门户不包含 X-FRAME-OPTIONS 标头。
- 云平台门户允许受影响的产品自行注册，无需创建账户。
- 当 web 应用程序信任的用户提交未经授权的命令时，受影响产品容易受到跨站点请求伪造的影响。
- 受影响的产品加密强度不足。
- 受影响的产品没有为产品的登录页面配置账户锁定策略。
- 受影响产品没有过滤器或签名检查来检测或阻止恶意文件上传到服务器。
- 受影响产品对来自帮助页面的客户端请求未执行足够的输入验证。

- 受影响产品容易被攻击者使用 ping 工具向其输入命令，从而受到攻击。
- 受影响产品容易被攻击者使用 traceroute 工具向其输入命令，从而受到攻击。
- 用于管理路由器的平台容易受到存储的跨站点脚本的攻击。
- 受影响的产品容易受到跨脚本攻击。
- 受影响产品的身份验证过程响应表明并验证存在用户名错误提示。
- 受影响的产品没有执行有效的密码策略。

受影响的产品

- IR615-S 路由器产品

受影响版本

- IR615-S 2.3.0.r5417 及之前的版本

解决措施

- 应下载更新的固件升级到版本 2.3.0.r5484，以防范潜在漏洞被利用，避免受到影响。
- 固件获取：请自行安全声明页下载固件，或者请联系映翰通技术支持或通过 support@inhand.com.cn 获取固件。

漏洞预防措施

映翰通网络为了保证产品完备的安全性，建议客户在使用产品的时候注重安全策略，包括但不限于以下内容：

1. 建议客户采取复杂和安全的用户名和密码机制，避免简单弱口令被暴力破解
2. 建议客户针对产品的管理采用加密方式访问，例如采用 HTTPS，关闭不必要的服务访问端口
3. 建议开启防火墙相关功能，保证产品和网络的安全性
4. 建议客户采用安全配置策略，例如访问控制，虚拟 IP，MAC 及 IP 地址绑定
5. 建议采取加密的数据传输方式等

首次发布日期

2021 年 11 月 2 日

资源

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

CVE-2021-38472 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38486 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38480 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38464 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38474 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38484 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38466 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38470 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38478 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38482 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38468 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38476 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38462 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

ICSA-21-280-01 - CISA ICS-CERT Advisories

联系我们

如果您有安全问题或疑虑，请通过 support@inhand.com.cn 或 010-84170010 联系映翰通网络。