产品安全公告

2026 年 06 月 18 日

InHand-PSA-2026-06

CVE-2026-38714, CVE-2026-38715,

CVE-2026-38716,CVE-2026-38717,

CVE-2026-38718

概述

映翰通网络针对 IR912，IR915 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。该产品存在某些安全漏洞，远程攻击者可利用这些漏洞在该产品上执行任意命令（获取 ROOT 权限）或造成拒绝服务攻击。

映翰通网络建议客户将对应设备型号固件版本更新至修复当前已知的安全漏洞的固件版本。

影响

- CVE-2026-38714:

  受影响产品的 Python 配置功能中存在一个命令注入漏洞，攻击者可通过该漏洞获取远程目标设备的 ROOT 权限。

- CVE-2026-38715 :

  受影响产品的日志查看功能中存在一个命令注入漏洞，攻击者可通过该漏洞获取远程目标设备的 ROOT 权限。

- CVE-2026-38716:

  受影响产品的 Python 应用导出功能中存在一个命令注入漏洞，攻击者可通过该漏洞获取远程目标设备的 ROOT 权限。

- CVE-2026-38717:
  受影响产品的文件上传功能中存在命令注入漏洞，攻击者可通过该漏洞获取远程目标设备的 ROOT 权限。
- CVE-2026-38718:
  受影响产品的设备注册功能中存在缓冲区溢出漏洞，攻击者可通过该漏洞对远程目标设备造成拒绝服务攻击。

受影响的产品和版本

- 工业路由器 IR912，固件版本 V1.0.0.r20042 及之前版本。
- 工业路由器 IR915，固件版本 V1.0.0.r20042 及之前版本。

解决措施

- IR912 下载并升级至 IR9-V1.0.0.r20044。
- IR915 下载并升级至 IR9-V1.0.0.r20044。

致谢

南京邮电大学的王锦程同学、于乐教授和香港理工大学的罗夏朴教授

首次发布日期

2026 年 06 月 18 日

资源

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