产品安全公告

2026 年 05 月 28 日

InHand-PSA-2026-05

CVE-2026-38702, CVE-2026-38703,

CVE-2026-38704,CVE-2026-38705,

CVE-2026-38707

概述

映翰通网络针对 IR302，IR305，IR315，IR615 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禁用安全功能、执行任意命令或任意删除文件。
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-2026-38702:
  受影响产品的管理控制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-2026-38703 :
  受影响产品的 ZeroTier VPN 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-2026-38704:
  受影响产品的 WireGuard VPN 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。

映翰通产品安全公告

- CVE-2026-38705:

  受影响产品的数字 I/O 功能中存在命令注入漏洞和缓冲区溢出漏洞，攻击者可通过该漏洞获取远程目标设备的 ROOT 权限或造成拒绝服务攻击。

- CVE-2026-38707:

  受影响产品的 IPSec VPN 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

受影响的产品和版本

- 工业路由器 IR302，固件版本 V3.5.108 及之前版本。
- 工业路由器 IR305，固件版本 V1.0.118 及之前版本。
- 工业路由器 IR315，固件版本 V1.0.118 及之前版本。
- 工业路由器 IR615，固件版本 V1.0.118 及之前版本。

解决措施

- IR302 下载并升级至 InRouter3XX-V3.5.112。
- IR305 下载并升级至 InRouter3X5-V1.0.121。
- IR315 下载并升级至 InRouter3X5-V1.0.121。
- IR615 下载并升级至 InRouter6XS-V1.0.121。

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 05 月 28 日

资源

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