产品安全公告

2022 年 5 月 10 日

InHand-PSA-2022-01

TALOS-2022-1468, TALOS-2022-1469, TALOS-2022-1470,
TALOS-2022-1471, TALOS-2022-1472, TALOS-2022-1473,
TALOS-2022-1474, TALOS-2022-1475, TALOS-2022-1476,
TALOS-2022-1477, TALOS-2022-1478, TALOS-2022-1481,
TALOS-2022-1495, TALOS-2022-1496, TALOS-2022-1499,
TALOS-2022-1500, TALOS-2022-1501

概述

映翰通网络针对工业路由器 IR302 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。该产品的 Web 及 CLI 配置存在安全漏洞，攻击者可通过这些漏洞进行非法远程代码执行、文件上传、权限提升以及盗取缓存等操作。

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讲固件升级至版本 InRouter3XX-V3.5.45，以修复当前已知的安全漏洞问题。

影响

- TALOS-2022-1468:
  CVSSv3 评分：9.9
  受影响的产品可通过某些 HTTP 请求进行任意文件上传。
- TALOS-2022-1469:
  CVSSv3 评分：5.4
  受影响的产品可通过某些 HTTP 请求执行任意 JavaScript 脚本。
- TALOS-2022-1470:
  CVSSv3 评分：7.5

受影响的产品 Web 界面中存在可被 JavaScript 访问的会话缓存，攻击者可通过 XSS 攻击盗取会话缓存。

- TALOS-2022-1471:
  CVSSv3 评分：8.2
  受影响的产品存在缓冲溢出漏洞，某些 API 指令可导致远程代码执行。
- TALOS-2022-1472:
  CVSSv3 评分：7.4
  受影响的设备存在配置导入漏洞，某些 HTTP 请求会导致权限提升。
- TALOS-2022-1473:
  CVSSv3 评分：9.9
  受影响的设备存在操作系统指令注入漏洞，某些 HTTP 请求会导致任意指令执行。
- TALOS-2022-1474:
  CVSSv3 评分：6.3
  受影响的设备存在配置导出漏洞，某些 HTTP 请求会导致权限提升。
- TALOS-2022-1475:
  CVSSv3 评分：9.1
  受影响的设备存在 CLI 注入漏洞，某些请求会执行非法命令。
- TALOS-2022-1476:
  CVSSv3 评分：9.1
  受影响的设备存在 CLI 堆栈缓冲溢出漏洞，某些恶意包会导致远程代码执行。
- TALOS-2022-1477:
  CVSSv3 评分：9.9
  受影响的设备存在 CLI 命令执行漏洞，某些请求会导致任意命令执行。
- TALOS-2022-1478:
  CVSSv3 评分：9.9
  受影响的设备存在操作系统命令注入漏洞，某些请求会导致任意命令执行。
- TALOS-2022-1481:
  CVSSv3 评分：9.9
  受影响的设备存在不恰当的输入认证，某些文件会导致远程代码执行。
- TALOS-2022-1495:
  CVSSv3 评分：9.9

受影响的产品存在固件升级漏洞，攻击者可通过特殊 HTTP 命令对设备进行固件升级。

- TALOS-2022-1496:
  CVSSv3 评分：4.3
  受影响的设备存在硬编码密码漏洞，某些网络请求会导致特权操作。
- TALOS-2022-1499:
  CVSSv3 评分：9.9
  受影响的设备存在指令注入漏洞，某些指令会导致远程代码执行。
- TALOS-2022-1500:
  CVSSv3 评分：9.9
  受影响的设备存在 CLI 堆栈缓冲区溢出漏洞，某些指令会导致远程代码执行。
- TALOS-2022-1501:
  CVSSv3 评分：9.9
  受影响的设备存在 CLI 缓冲溢出漏洞，某些网络请求会导致远程代码执行。

受影响的产品

- IR302 路由器产品

受影响版本

- 工业路由器 IR302 固件版本 3.5.37 及之前版本

解决措施

- 下载并升级固件至 3.5.45 版本

首次发布日期

2022 年 5 月 11 日

资源

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