产品安全公告

2022 年 10 月 25 日

InHand-PSA-2022-02

TALOS-2022-1518, TALOS-2022-1519, TALOS-2022-1520,
TALOS-2022-1521, TALOS-2022-1522, TALOS-2022-1523

概述

映翰通网络针对 IR302 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固件版本升级至 InRouter3XX-V3.5.56，以修复当前已知的安全漏洞。

影响

- TALOS-2022-1518:
  CVSSv3 评分：4.9
  受影响产品的 console 命令 nvram 存在漏洞，攻击者可使用一系列特殊网络请求禁用安全功能。
- TALOS-2022-1519:
  CVSSv3 评分：4.3
  受影响产品的 console 命令 infct 存在漏洞，攻击者可使用一系列特殊网络请求执行任意命令。
- TALOS-2022-1520:
  CVSSv3 评分：6.5
  受影响产品的 console 命令 verify 存在漏洞，攻击者可使用一系列特殊网络请求禁用安全功能。

映翰通产品安全公告

- TALOS-2022-1521:
  CVSSv3 Score 6.5
  受影响产品的 console 命令 support 存在漏洞，攻击者可使用一系列特殊网络请求执行任意命令。
- TALOS-2022-1522:
  CVSSv3 Score 6.5
  受影响产品的 upload.cgi 功能（ httpd，端口 4444 ）存在漏洞，攻击者可使用一系列特殊 HTTP 请求删除任意文件。
- TALOS-2022-1523:
  CVSSv3 Score 7.4
  受影响产品对漏洞 TALOS-2022-1472 和 TALOS-2022-1474 修复不完全，攻击者仍然可以通过这些漏洞进行特权升级或信息泄露。

受影响的产品和版本

- 工业路由器 IR302，固件版本 3.5.45 及之前版本。

解决措施

- 下载并升级至 InRouter3XX-V3.5.56。

首次发布日期

2022 年 10 月 25 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