Product Security Advisory

May 10, 2022

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

Overview

InHand Networks has confirmed the vulnerabilities impacting the Industrial Router IR302, which will allow attackers to execute arbitrary commands, file uploading, increase privileges or steal cookies via specific request.

Customers should upgrade to version InRouter3XX-V3.5.45 to prevent these problems.

Impact

- TALOS-2022-1468:
  CVSSv3 Score 9.9
  The affected product can allow arbitrary file upload via specific HTTP request.
- TALOS-2022-1469:
  CVSSv3 Score 5.4
  The affected product can allow arbitrary JavaScript execution via specific HTTP request.
- TALOS-2022-1470:
  CVSSv3 Score 7.5

The affected product has vulnerability in web interface session cookies which is accessible via JavaScript that allow an attacker to perform an XSS attack to steal session cookies.

- TALOS-2022-1471:
  CVSSv3 Score 8.2
  The affected product has a buffer overflow vulnerability that will lead to remote code execution via specific API request.
- TALOS-2022-1472:
  CVSSv3 Score 7.4
  The affected product has configuration import vulnerability that a specific HTTP request can lead to increased privileges.
- TALOS-2022-1473:
  CVSSv3 Score 9.9
  The affected product has OS command injection that will lead to arbitrary command execution via specific HTTP request.
- TALOS-2022-1474:
  CVSSv3 Score 6.3
  The affected product has configuration export vulnerability that a specific HTTP request can lead to increased privileges.
- TALOS-2022-1475:
  CVSSv3 Score 9.1
  The affected product has injection vulnerability in a console command that will lead to command execution via specific sequence of request.
- TALOS-2022-1476:
  CVSSv3 Score 9.1
  The affected product has stack-based buffer overflow vulnerability in a console command that will lead to remote code execution via specific sequence of malicious packets.
- TALOS-2022-1477:
  CVSSv3 Score 9.9
  The affected product has command execution vulnerability in a console command that will lead to arbitrary command execution via specific sequence of request.

- TALOS-2022-1478:
  CVSSv3 Score 9.9
  The affected product has command injection vulnerability in an OS command that will lead to arbitrary command execution via specific sequence of request.
- TALOS-2022-1481:
  CVSSv3 Score 9.9
  The affected product has an improper input validation vulnerability that will lead to remote code execution via a specific-crafted file.
- TALOS-2022-1495:
  CVSSv3 Score 9.9
  The affected product has firmware upgrade vulnerability that will lead to firmware upgrade via a specific sequence of HTTP request.
- TALOS-2022-1496:
  CVSSv3 Score 4.3
  The affected product has a hard-coded password vulnerability that will lead to execute privileged operation via a specific sequence of network request.
- TALOS-2022-1499:
  CVSSv3 Score 9.9
  The affected product has command injection vulnerability in console that will lead to remote code execution via a specific sequence of request.
- TALOS-2022-1500:
  CVSSv3 Score 9.9
  The affected product has stack-based buffer overflow vulnerability in console that will lead to remote code execution via a specific sequence of request.
- TALOS-2022-1501:
  CVSSv3 Score 9.9
  The affected product has buffer overflow vulnerability in console that will lead to remote code execution via a specific sequence of network request.

Affected Versions

- IR302 version 3.5.37 and prior.

Mitigation

- Upgrade to version 3.5.45

Initial Publication Date

May 10th, 2022

Resources

Security Solutions Website - https://inhandnetworks.com/product-security-advisories.html
https://talosintelligence.com/vulnerability_reports#zerodays