Talos Vulnerability Report

TALOS-2022-1472

InHand Networks InRouter302 router configuration import privilege escalation vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-21182

Summary

A privilege escalation vulnerability exists in the router configuration import functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.4

Product URLs

InRouter302 - https://www.inhandnetworks.com/products/inrouter300.html

CVSSv3 Score

7.4 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

CWE

CWE-284 - Improper Access Control

Details

The InRouter302 is an industrial LTE router. It features remote management functionalities and several security protection mechanism, such as: VPN technologies, firewall functionalities, authorization management and several other features.

The inRouter302 offers the possibility to have non-privileged users. These non-privileged users, allegedly, should not be able to perform certain actions. But a non-privileged user is allowed to import the router configuration, through the `upload.cgi` API, effectively allowing the user to change the privileged user credentials.

Vendor Response

The vendor has updated their website and uploaded the latest firmware on it. https://inhandnetworks.com/product-security-advisories.html https://www.inhandnetworks.com/products/inrouter300.html#link4

https://www.inhandnetworks.com/upload/attachment/202205/10/InHand-PSA-2022-01.pdf

Timeline

2022-03-02 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
