Talos Vulnerability Report

TALOS-2022-1495

InHand Networks InRouter302 iburn firmware checks firmware update vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-26510

Summary

A firmware update vulnerability exists in the iburn firmware checks functionality of InHand Networks InRouter302 V3.5.37. A specially-crafted HTTP request can lead to firmware update. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.37

Product URLs

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

CVSSv3 Score

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

CWE

CWE-347 - Improper Verification of Cryptographic Signature

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, through the `upgrade.cgi` API, the upgrade of its firmware. The upgrade process does not include any cryptographic signature that would guarantee that the content of the upgrade is legitimate. This would allow any attacker, able to perform the `upgrade.cgi` API, to insert backdoor and modify the firmware of the router. The same consequences are true for an attacker able to perform a man-in-the-middle attack, where the attacker would wait for a legitimate user to initiate a firmware update, then modify the firmware in-transit. The `iburn` binary, the one responsible for performing the actual firmware update, only calculates and checks a CRC32.

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

2022-03-23 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
