Product Security Advisory

March 14, 2023

InHand-PSA-2023-03

FG-VD-22-101, FG-VD-22-106, FG-VD-22-107,

FG-VD-22-108, FG-VD-22-109

Overview

InHand Networks has confirmed the vulnerabilities impacting Industrial Router InRouter615-S version V2.3.0.r5542 and prior, which attackers can use to perform operations such as denial of service, account information acquisition, and login brute force on the affected device.

Customers should upgrade affected devices to version InRouter6XX-S-V2.3.0.r5550 to prevent these problems.

Impact

- FG-VD-22-101:

  CVSSv3 Score 6.5

  The affected product has a vulnerability in the apply.cgi interface due to a lack of strict input parameter filtering, resulting in Denial of Service from non-formatted inputs.
- FG-VD-22-106:

  CVSSv3 Score 6.5

The affected product is vulnerable to password leakage due to the lack of encryption for passwords.

- FG-VD-22-107:
- CVSSv3 Score 5.3

  The affected product has no login restrictions on SSH, which allows attackers to perform brute force attacks.
- FG-VD-22-108:

  CVSSv3 Score 8.8

  The affected product has an XSS vulnerability in the OpenVPN configuration page.
- FG-VD-22-109:

  CVSSv3 Score 8.8

  The affected product has an XSS vulnerability in the IPSec Tunnels configuration page.

Affected Versions

- InRouter615-S version InRouter6XX-S-V2.3.0.r5542 and prior.

Mitigation

- Upgrade to version InRouter6XX-S-V2.3.0.r5550.

Acknowledgements

Zhouyuan Yang of Fortinet's FortiGuard Labs.

Initial Publication Date

Resources

Security Solutions Website - https://inhandnetworks.com/product-security-advisories.html

https://fortiguard.com/zeroday