Product Security Advisory

November 1, 2021

InHand-PSA-2021-01

CVE-2021-38472, CVE-2021-38486, CVE-2021-38480,
CVE-2021-38464, CVE-2021-38474, CVE-2021-38484,
CVE-2021-38466, CVE-2021-38470, CVE-2021-38478,
CVE-2021-38482, CVE-2021-38468, CVE-2021-38476,
CVE-2021-38462

ICSA-21-280-01

Overview

InHand Networks has confirmed the vulnerabilities impacting the IR615-S Router. A web GUI in the router product which is a user-friendly UI to config the router used a weak password policy, Cross-site Scripting, Inadequate Encryption Strength. Customers should upgrade to version InRouter6XX-S-V2.3.0.r5484.

Impact

- The IR615-S's management portal does not contain an X-FRAME-OPTIONS header.
- The vendor's cloud portal allows for self-registration of the affected product without any requirements to create an account.
- The affected product is vulnerable to cross-site request forgery when unauthorized commands are submitted from a user the web application trusts.
- The affected product has inadequate encryption strength.
- The affected product has no account lockout policy configured for the login page of the product.
- The affected product does not have a filter or signature check to detect or prevent an upload of malicious files to the server.

- The affected product does not perform sufficient input validation on client requests from the help page.
- The affected product is vulnerable to an attacker using a ping tool to inject commands into the device.
- The affected product is vulnerable to an attacker using a traceroute tool to inject commands into the device.
- The affected product's website used to control the router is vulnerable to stored cross-site scripting.
- The affected product is vulnerable to stored cross-scripting.
- The affected product's authentication process response indicates and validates the existence of a username.
- The affected product does not enforce an efficient password policy.

Affected Versions

- IR615-S version 2.3.0.r5417 and prior.

Mitigation

- Upgrade to version 2.3.0.r5484

Initial Publication Date

November 2nd, 2021

Resources

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

CVE-2021-38472 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38486 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38480 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38464 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38474 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38484 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38466 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38470 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38478 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38482 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38468 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38476 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

CVE-2021-38462 - NIST National Vulnerability Database (NVD) and MITRE CVE® List

ICSA-21-280-01 - CISA ICS-CERT Advisories