



CVE-2021-38466

Published on: 10/19/2021 12:00:00 AM UTC

Last Modified on: 10/22/2021 02:45:00 PM UTC

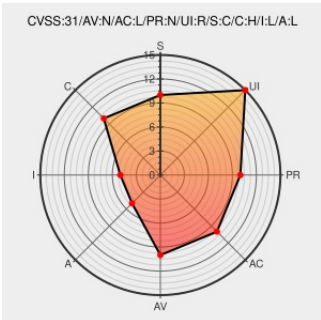
CVE-2021-38466 - advisory for ICSA-21-280-05

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Ir615** from **Inhandnetworks** contain the following vulnerability:

InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not perform sufficient input validation on client requests from the help page. This may allow an attacker to perform a reflected cross-site scripting attack, which could allow an attacker to run code on behalf of the client browser.

CVE-2021-38466 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [InHand Networks](#) - **IR615 Router** version = **2.3.0.r4724** and **2.3.0.r4870**

Vulnerability Patch/Work Around

InHand Networks has not responded to requests to work with CISA to mitigate these vulnerabilities. Users of this affected product are invited to contact InHand Networks customer support.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
InHand Networks IR615 Router CISA	us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/advisories/icsa-21-280-05

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590971 InHand Networks IR615 Router (Update A) Multiple Vulnerabilities (ICSA-21-280-05)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Inhandnetworks	Ir615	-	All	All	All
Operating System	Inhandnetworks	Ir615 Firmware	2.3.0.r4724	All	All	All
Operating System	Inhandnetworks	Ir615 Firmware	2.3.0.r4870	All	All	All

`cpe:2.3:h:inhandnetworks:ir615:-:*:*:*:*:*:`

`cpe:2.3:o:inhandnetworks:ir615_firmware:2.3.0.r4724:*:*:*:*:*:`

`cpe:2.3:o:inhandnetworks:ir615_firmware:2.3.0.r4870:*:*:*:*:*:`

Discovery Credit

Haviv Vaizman, Hay Mizrachi, Alik Koldobsky, Ofir Manzur, and Nikolay Sokolik of OTORIO reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
@management_sun	IT Risk:(Including Critical)複数のMobile Industrial Robots製品における複数の脆弱性 -2/3 CVE-2021-38484(CVSSv3=9.1) CVE-2021-38466(... twitter.com/i/web/status/1...	2021-10-08 10:44:06
@management_sun	IT Risk:InHand Networks製ルーターIR615に複数の脆弱性 -3/4 CVE-2021-38466 OSコマンドインジェクション (CWE-78) - CVE-2021-38470、CVE-2021-3847... twitter.com/i/web/status/1...	2021-10-15 02:31:43
@CVEreport	CVE-2021-38466 : InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not perform sufficient inpu... twitter.com/i/web/status/1...	2021-10-19 13:04:17

[← Previous ID](#)

[Next ID →](#)

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)