



CVE-2022-21809

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-21809
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-12 17:15:00 UTC
Updated	2022-05-23 18:38:00 UTC
Description	A file write vulnerability exists in the httpd upload.cgi functionality of InHand Networks InRouter302 V3.5.4. A specially-craft

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Inhandnetworks	Inrouter302	-	All	All	All
Operating System	Inhandnetworks	Inrouter302 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
TALOS-2022-1468 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
www.inhandnetworks.com/upload/attachment/202205/10/InHand-PSA-2022-01.pdf	CONFIRM	www.inhandnetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591033](#) InHand Networks Industrial Router IR302 Multiple Vulnerabilities (InHand-PSA-2022-01)

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](#).

Free CVE JSON API [cve.report/api](#)

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