



CVE-2018-5447

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

Summary

CVE	CVE-2018-5447
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-25 22:29:00 UTC
Updated	2019-10-09 23:41:00 UTC
Description	An Improper Input Validation issue was discovered in Nari PCS-9611 relay. An improper input validation vulnerability has been discovered in the Nari PCS-9611 relay. The vulnerability is located in the Nari PCS-9611 relay's firmware. The vulnerability is a buffer overflow that can be triggered by sending a specially crafted packet to the relay. The vulnerability is a buffer overflow that can be triggered by sending a specially crafted packet to the relay. The vulnerability is a buffer overflow that can be triggered by sending a specially crafted packet to the relay.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nrec	Pcs-9611	-	All	All	All
Hardware	Nrec	Pcs-9611	-	All	All	All
Operating System	Nrec	Pcs-9611 Firmware	-	All	All	All
Operating System	Nrec	Pcs-9611 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Nari PCS-9611 (Update A) CISA	MISC	ics-cert.us-cert.gov	Third Party Advisory, US Government Resource
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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