



CVE-2018-10123

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

Summary

CVE	CVE-2018-10123
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-16 13:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	p910nd on Inteno IOPSYS 2.0 through 4.2.0 allows remote attackers to read, or append data to, arbitrary files via requests

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intenogroup	lophys	-	All	All	All
Hardware	Intenogroup	lophys	-	All	All	All
Operating System	Intenogroup	lophys Firmware	All	All	All	All

References

Reference	Source	Link	Tags
pwn910nd - abusing OpenWRT's printer server to become root	MISC	neonsea.uk	Explo
Inteno IOPSYS 2.0 < 4.2.0 - 'p910nd' Remote Command Execution - Hardware remote Exploit	EXPLOIT-DB	www.exploit-db.com	Explo
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

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