CVE-2022-3203

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-3203
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-21 13:15:00 UTC
Updated	2022-12-07 03:16:00 UTC
Description	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled.

Risk And Classification

Problem Types: CWE-912

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Oringnet	Iap-420	-	All	All	All
Hardware	Oringnet	Iap-420	-	All	All	All
Operating System	Oringnet	Iap-420 Firmware	2.0m	All	All	All
Operating System	Oringnet	Iap-420 Firmware	2.0m	All	All	All

References

Reference	Source	Link	Ta
LORD OF THE ORINGS (CVE-2022-3203): Vulnerability Analysis of an Industrial Access Point – MADS lab	CONFIRM	mads.uniud.it	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

LEGACY: Lorenzo Bazzana and Marino Miculan of Università degli studi di Udine, Michele Codutti of Danieli Automation

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