



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	lap-420	-	All	All	All
Hardware	Oringnet	lap-420	-	All	All	All
Operating System	Oringnet	lap-420 Firmware	2.0m	All	All	All
Operating System	Oringnet	lap-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.

© [CVE.report](#) 2026 |

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](#).

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

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