



CVE-2023-5296

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

Summary

CVE	CVE-2023-5296
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-29 22:15:00 UTC
Updated	2023-11-07 04:23:00 UTC
Description	A vulnerability was found in Xinhua RockOA 1.1/2.3.2/15.X3amdi and classified as problematic. Affected by this issue is som

Risk And Classification

Problem Types: CWE-640

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rockoa	Rockoa	1.1	All	All	All
Application	Rockoa	Rockoa	15.x3amdi	All	All	All
Application	Rockoa	Rockoa	2.3.2	All	All	All

References

Reference	Source	Link	T
Login required	MISC	vuldb.com	
CVE-2023-5296: Xinhua RockOA Password password recovery	MISC	vuldb.com	
Any user's password modification vulnerability in Xinhua OA V2.3.2 · Issue #1 · magicwave18/vuldb · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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](#)