



CVE-2023-30403

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

Summary

CVE	CVE-2023-30403
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-02 20:15:00 UTC
Updated	2023-05-10 16:47:00 UTC
Description	An issue in the time-based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows

Risk And Classification

Problem Types: CWE-613

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Aigital	Wireless-n Repeater Mini Router	-	All	All	All
Operating System	Aigital	Wireless-n Repeater Mini Router Firmware	0.131229	All	All	All

References

Reference	Source	Link	Tags
dl.packetstormsecurity.net/2305-exploits/aigitalwnr-bypass.txt	MISC	dl.packetstormsecurity.net	
Route to RCE - Dissecting a cheap WiFi repeater	MISC	mandomat.github.io	
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.

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