CVE-2016-4824

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

Summary

CVE	CVE-2016-4824
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-25 21:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Wi-Fi Protected Setup (WPS) implementation on Corega CG-WLR300GNV and CG-WLR300GNV-W devices does not

Risk And Classification

Primary CVSS: v3.0 5.3 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Problem Types: CWE-254 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Corega	Cg-wlr300gnv	-	All	All	All
Hardware	Corega	Cg-wlr300gnv-w	-	All	All	All
Operating System	Corega	Cg-wlr300gnv-w Firmware	-	All	All	All
Operating System	Corega	Cg-wlr300gnv Firmware	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
jvndb.jvn.jp/jvndb/JVNDB-2016-000109	af854a3a-2127-422b-91ae-364da2661108	jvndb.jvn.jp
販売終了商品｜コレガ	af854a3a-2127-422b-91ae-364da2661108	corega.jp
JVN#75028871: CG-WLR300GNV Series does not limit authentication attempts	af854a3a-2127-422b-91ae-364da2661108	jvn.jp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report