Predictable Default Cryptographic Key Used for DES Encryption in TP-Link TL-WL841N

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

Summary

CVE	CVE-2026-5039
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 18:16:30 UTC
Updated	2026-04-23 18:16:30 UTC
Description	TP-Link TL-WR841N v13 uses DES-CBC encryption in the TDDPv2 debug protocol with a cryptographic key derived from c

Risk And Classification

Primary CVSS: v4.0 6.1 MEDIUM from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-1394 | CWE-1394 CWE-1394 Use of default cryptographic key

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	6.1	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:
4.0	CNA	CVSS	6.1	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	TL-WL841N V13	affected 0.9.1 Build 20231120 Rel.62366 custom	Not specified

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/download/tl-wr841n/v13	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
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.