Command Injection in Wireless Control CLI on TP-Link Archer NX200, NX210, NX500 and NX600

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-15518
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 18:16:23 UTC
Updated	2026-03-31 19:05:01 UTC
Description	Improper input handling in a wireless-control administrative CLI command on TP-Link Archer NX200, NX210, NX500 and N

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/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-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	8.5	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer Nx200	3.0	All	All	All
Operating System	Tp-link	Archer Nx200 Firmware	All	All	All	All
Hardware	Tp-link	Archer Nx210	3.0	All	All	All
Operating System	Tp-link	Archer Nx210 Firmware	All	All	All	All

Hardware	Tp-link	Archer Nx500	2.0	All	All	All
Operating System	Tp-link	Archer Nx500 Firmware	All	All	All	All
Hardware	Tp-link	Archer Nx600	3.0	All	All	All
Operating System	Tp-link	Archer Nx600 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Archer NX600 V3.0	affected 1.3.0 Build 260309 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX600 V2.0	affected 1.3.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX600 V1.0	affected 1.4.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX500 V2.0	affected < 1.5.0 Build 260309 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX500 V1.0	affected 1.3.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX210 V3.0	affected 1.3.0 Build 260309 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX210 V2.0 V2.20	affected 1.3.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX200 V3.0	affected < 1.3.0 Build 260309 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX200 V2.20	affected 1.3.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX200 V2.0	affected 1.3.0 Build 260311 custom	Linux
CNA	TP-Link Systems Inc.	Archer NX200 V1.0	affected 1.8.0 Build 260311 custom	Linux

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/faq/5027	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
www.tp-link.com/en/support/download/archer-nx210	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/en/support/download/archer-nx500	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/en/support/download/archer-nx600	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/en/support/download/archer-nx200	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Saifeldeen Aziz from Cyshield (en)

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

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