



TOTOLINK CA300-PoE upgrade.so setUpgradeUboot os command injection

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2025-6620
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-25 18:15:25 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been rated as critical. Affected by this issue is the func

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@vulldb.com

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

Problem Types: CWE-77 | CWE-78 | CWE-78 OS Command Injection | CWE-77 Command Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C..
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C: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

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Totolink	Ca300-poe	-	All	All	All
Operating System	Totolink	Ca300-poe Firmware	6.2c.884	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	TOTOLINK	CA300-PoE	affected 6.2c.884	Not specified

References			
Reference	Source	Link	Tags
github.com/wudipjq/my_vuln/blob/main/totolink4/vuln_46/46.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Third Party /
vuldb.com	cna@vuldb.com	vuldb.com	Permissions
vuldb.com	cna@vuldb.com	vuldb.com	Third Party /
www.totolink.net	cna@vuldb.com	www.totolink.net	Product
github.com/wudipjq/my_vuln/blob/main/totolink4/vuln_46/46.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Third Party /
vuldb.com	cna@vuldb.com	vuldb.com	Third Party /
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative



Vendor Comments And Credit

CNA: pjqwudi (VulDB User) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2025-06-25T00:00:00.000Z	Advisory disclosed
CNA	2025-06-25T02:00:00.000Z	VulDB entry created
CNA	2025-06-25T09:19:10.000Z	VulDB entry last update

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