contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TOTOLINK CA300-PoE: new CVE

CVE-2026-123957 · record published 7 November 2026

Analysis Report

Anyone running TOTOLINK CA300-PoE on firmware 6.2c.884 should act now: the record scores this 9.9 and states the exploit is publicly available, with no fixed firmware recorded. Check whether the …

PREPARED BY	NamiQ	DATE	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/totolink-ca300-poe-cve-2026-123957

The bottom line

> *Anyone running TOTOLINK CA300-PoE on firmware 6.2c.884 should act now: the record scores this 9.9 and states the exploit is publicly available, with no fixed firmware recorded. Check whether the management interface is reachable from outside your network and block that access immediately.*

At a glance

Fact	Detail
Product	TOTOLINK CA300-PoE (CVE-2026-123957)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by VulDB on 7 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 8 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone running a TOTOLINK CA300-PoE on firmware 6.2c.884. The record names only that version; no other firmware is listed as affected or unaffected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you have a TOTOLINK CA300-PoE on your network?	Nothing to do for this CVE.	Check the firmware version.
Is the firmware version 6.2c.884?	The record does not name your version as affected.	Check whether the management interface is reachable from outside your network.
Is the device's management interface reachable from outside your internal network?	Restrict management access to trusted hosts only and await a vendor patch.	Block that access immediately and await a vendor patch.

What it is

An attacker who can reach the device's web management interface can send a crafted value for the ipStart argument to the setIpQosRules function, causing a buffer overflow. The record scores this 9.9 and states the exploit has been publicly disclosed and may be utilised.

Things people will get wrong

- Installing a firmware update will resolve this No fixed firmware version is recorded. The record lists no unaffected release. Do not assume any update resolves this until a vendor advisory confirms it.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the firmware version on every TOTOLINK CA300-PoE

- Log in to each device's management page and note the firmware version shown on the status or system information screen.
- The record names only 6.2c.884 as affected; compare what you find to that string exactly.

```
cat /etc/openwrt_release
```

Step 2: Check whether the management interface is externally reachable

- Confirm whether the device's HTTP or HTTPS management port is accessible from outside your internal network.
- If it is, block that access at your firewall before taking any other step.

Step 3: Restrict management access to trusted hosts only

- Limit access to the management interface to known administrator IP addresses or a dedicated management VLAN.
- This reduces the attack surface while you wait for a vendor patch.

Step 4: Watch for a vendor firmware patch

- No fixed firmware is recorded at time of writing; monitor the TOTOLINK support page for CA300-PoE firmware updates.
- When a patched version is released, apply it and confirm the firmware version changed.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of a severe vulnerability in the TOTOLINK CA300-PoE (CVE-2026-123957), published 7 November 2026. The flaw is in the device's web management interface, affects firmware 6.2c.884, and can be exploited remotely. The exploit has been publicly disclosed. The record scores this 9.9. No fixed firmware is currently recorded. Please confirm: whether we run any TOTOLINK CA300-PoE devices and on which firmware; whether the management interface of any such device is reachable from outside our internal network; and whether that access can be blocked while we await a vendor patch. We would like written confirmation of your findings and any actions taken by [date].*

The weakness behind it

The record classes this as CWE-120 and CWE-119.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a web CGI endpoint reachable over the network; exploiting it would likely follow the pattern of targeting a public-facing application to gain initial access to the device.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Buffer overflows in CGI handlers on embedded devices typically yield arbitrary command execution; a successful exploit would likely result in commands running on the device.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *A vulnerability was determined in TOTOLINK CA300-PoE 6.2c.884. Impacted is the function setIpQosRules of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument ipStart causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.*

Versions of TOTOLINK CA300-PoE the record lists as affected:

- 6.2c.884

The record gives no version ranges. Use the vendor's advisory for the affected versions.

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-123957
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on

it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-123957
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Whether a patched firmware version exists or when TOTOLINK plans to release one for the CA300-PoE.
- Whether the vulnerable function requires authentication to reach, or whether it is accessible before login.
- Whether firmware versions other than 6.2c.884 are affected; the record names only that version.
- What level of access a successful exploit provides — the record confirms buffer overflow but does not state the resulting outcome.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 8 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-123957: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:X/RC:C` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
7 November 2026	CVE record published by VulDB.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
TOTOLINK CA300-PoE on 6.2c.884 with management interface reachable from the internet	Medium	Immediately
TOTOLINK CA300-PoE on 6.2c.884 with management reachable from untrusted internal hosts	Medium	This week
TOTOLINK CA300-PoE on 6.2c.884 with management restricted to a trusted admin segment	Medium	Next patch cycle, or when a vendor fix is available
TOTOLINK CA300-PoE on the network but not running 6.2c.884	Low	Monitor for vendor guidance on affected versions

No TOTOLINK CA300-PoE on the network	None	None for this CVE

Appendix 4. Definition of done

- Every TOTOLINK CA300-PoE you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-123957: https://www.cve.org/CVERecord?id=CVE-2026-123957
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432020
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432020/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-123957