

## SECURITY ADVISORY

# mqtttnet thinglinks: new CVE

CVE-2026-62853 · record published 30 October 2026

## Analysis Report

If you run ThingLinks, update to 1.4.0 this week and first find out who can log in to it.  
If you do not run ThingLinks, you can stop reading.

|             |                               |         |                                                            |
|-------------|-------------------------------|---------|------------------------------------------------------------|
| PREPARED BY | NamiQ                         | DATE    | 31 October 2026                                            |
| FACTS AS OF | 31 October 2026               | VERSION | 1.0                                                        |
| SEVERITY    | <b>Critical: CVSS 3.1 9.9</b> | STATUS  | Not on CISA's exploited list;<br>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/mqtttnet-thinglinks-cve-2026-62853](https://namiq.io/insights/mqtttnet-thinglinks-cve-2026-62853)

# The bottom line

*If you run ThingLinks, update to 1.4.0 this week and first find out who can log in to it. If you do not run ThingLinks, you can stop reading.*

# At a glance

| Fact            | Detail                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product         | mqttpsnet thinglinks (CVE-2026-62853)                                                                                                                                                                      |
| Severity        | Critical: 9.9 (CVSS 3.1)                                                                                                                                                                                   |
| Status          | A new CVE record, published by GitHub on 30 October 2026. Not on CISA's list of exploited vulnerabilities when we read it on 31 October 2026, which means nothing public says yet that anyone is using it. |
| Fixed in        | ThingLinks 1.4.0 (released 22 July 2026, per the project's release notes)                                                                                                                                  |
| Who looks first | Anyone who runs the ThingLinks IoT platform at a version below 1.4.0, especially where the admin console or API can be reached from the internet or by many staff, partners or customers.                  |

# Does this apply to you?

Answer in order. Stop at the first no.

| Question                                                        | If no                                                           | If yes                                         |
|-----------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------|
| Do you or your IT provider run ThingLinks (mqttpsnet) anywhere? | Nothing to do for this CVE.                                     | Check the version (next question).             |
| Is the version below 1.4.0?                                     | 1.4.0 or later is the fixed line; record the version.           | You are in range. Go to the next question.     |
| Can anyone untrusted, or a low-privilege account, log in to it? | Lower urgency, but still update. Staff accounts can be misused. | Treat as urgent: restrict access, then update. |

## What it is

---

A logged-in user of ThingLinks can send their own Groovy code to the rule engine's script test endpoint. The server compiles and runs it with no sandbox, so the attacker can run any code on the server.

## Why it matters

---

The score is 9.9. The vendor's advisory says the attacker needs only a low-privilege login, over the network, with no user interaction. The 'scope changed' rating means a hit can reach beyond ThingLinks itself. Our reading is that a server running attacker code can expose device data and the network behind it. The same release also fixes CVE-2026-62849, so update once for both.

## What the vendor's advisory says

---

We read two pages on [github.com](https://github.com). In short:

- The vendor's advisory was published 27 June 2026 and rates the flaw Critical, 9.9. It lists CWE-78 and CWE-94.
- The advisory names the affected package as thinglinks-rule and says versions below 1.4.0 are affected; 1.4.0 is the patched version.
- The release notes for 1.4.0 (22 July 2026) say the fix removes externally reachable test controllers and limits dynamic execution to internal service calls.
- The same release fixes CVE-2026-62849, an unauthenticated SQL injection in the TDengine TDS APIs.
- The release also moves the shared thinglinks-parent and thinglinks-util dependency line to 1.0.8.3 and replaces bundled credentials with placeholders.

## Things people will get wrong

---

- "It needs a login, so it is not urgent." The record says a low-privilege login is enough, and the vendor rates it 9.9. Any account that can reach the endpoint is a route in.
- "Not on the CISA list, so nobody is using it." CISA's list did not include it when read. That says nothing about whether anyone is trying it.
- "The earlier ThingLinks fix covers it." The vendor names 1.4.0 as the fixed version for this flaw. Versions below it are affected.

The wording includes conditions the score may not show: authenticated. Read the record before you decide it does not apply to you.

## 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 where ThingLinks runs and which version

---

- Ask your IT provider, or check your servers and containers, for ThingLinks or the thinglinks-rule package.
- Record each version. Anything below 1.4.0 is affected, per the record.

```
docker ps --format '{{.Names}} {{.Image}}'
docker images | grep -i thinglinks
```

## Step 2: Reduce who can reach it

---

- Keep the admin console and API off the internet where you can, for example behind a VPN.
- Review which accounts exist and remove ones nobody needs, since any login can be used.

## Step 3: Update to 1.4.0

---

- Move to ThingLinks 1.4.0, which the vendor names as the fixed version.
- This also closes CVE-2026-62849. Take a backup first and note that the release is a large one.

## Step 4: Confirm the fix and look for misuse

---

- Check the running version is 1.4.0 or later and write it down.
- Look at the activity listed under what to look for.

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.

*Hello. We need to check our exposure to CVE-2026-62849 and CVE-2026-62853 in ThingLinks (mqtsnet). The second lets a logged-in user run code on the server through the Groovy script test endpoint in versions below 1.4.0. Please tell us whether we run ThingLinks, where, and which version. If it is below 1.4.0, please update to 1.4.0, the version the vendor names as fixed, and tell us who can log in. Please confirm the version and the fix in writing by the date you agree with us. Thank you.*

## The weakness behind it

---

The record classes this as CWE-78 and CWE-94.

## The sources, in their words

---

The CVE record:

*ThingLinks is an enterprise IoT platform. Prior to 1.4.0, the `/groovyScriptTest/registerScript` endpoint accepts user-supplied Groovy script content and passes it to an unsandboxed `Groovy compilation and loading` flow. An authenticated attacker can provide code that is compiled and instantiated on the server, resulting in arbitrary server-side code execution. The issue affects the `rule engine`'s Groovy script test/register flow. This issue is fixed in version 1.4.0.*

Versions of mqtsnet thinglinks the record lists as affected:

- < 1.4.0

## What we do not know yet

---

- The sources do not say whether the flaw is being exploited. CISA did not list it when read.
- They do not say whether any configuration, other than having an account, limits who can reach the endpoint.
- They do not name any workaround short of updating to 1.4.0.
- They do not say how to tell whether a server has already been attacked.
- 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 31 October 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "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-2026-62853:** score 9.9, CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H 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                           |
|-----------------|---------------------------------|
| 30 October 2026 | CVE record published by GitHub. |

## 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                           |
|-----------------------------------------------------------------------------------|----------|-------------------------------------|
| Version below 1.4.0, reachable from the internet, with accounts for outside users | High     | Within days; restrict access now    |
| Version below 1.4.0, internal network only, several staff accounts                | Medium   | This week                           |
| Version below 1.4.0, only one or two trusted administrators can log in            | Medium   | Next patch cycle, soon              |
| Version 1.4.0 or later                                                            | Low      | Record the version; nothing further |
| You do not run ThingLinks                                                         | None     | None for this CVE                   |

## Appendix 4. Definition of done

---

- Every mqtttsnet thinglinks 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-2026-62853: <https://www.cve.org/CVERecord?id=CVE-2026-62853>
- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Advisory or release notes read: [github.com/mqttsnet/thinglinks/security/advisories/GHSA-9v](https://github.com/mqttsnet/thinglinks/security/advisories/GHSA-9v): <https://github.com/mqttsnet/thinglinks/security/advisories/GHSA-9vph-5ccx-qp9v>
- Advisory or release notes read: [github.com/mqttsnet/thinglinks/releases/tag/v1.4.0](https://github.com/mqttsnet/thinglinks/releases/tag/v1.4.0): <https://github.com/mqttsnet/thinglinks/releases/tag/v1.4.0>
- Reference in the CVE record: [github.com](https://github.com/mqttsnet/thinglinks/commit/311ee760dad798f48652722989fcea02349e13a3): <https://github.com/mqttsnet/thinglinks/commit/311ee760dad798f48652722989fcea02349e13a3>