contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Netis WF2409E: new CVE

**CVE-2026-136136 · record published 24 November 2026**

## Analysis Report

Any owner of a Netis WF2409E running firmware 20261026 or earlier should act now — no patch is recorded and an exploit is publicly available. As a first step, block access to the router's web …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 25 November 2026 |
| FACTS AS OF | 25 November 2026 | VERSION | 1.0 |
| SEVERITY | **Critical: CVSS 4.0 10.0** | 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/netis-wf2409e-cve-2026-136136

## The bottom line

> *Any owner of a Netis WF2409E running firmware 20261026 or earlier should act now — no patch is recorded and an exploit is publicly available. As a first step, block access to the router's web management interface from untrusted networks.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Netis WF2409E (CVE-2026-136136) |
| Severity | Critical: 10 (CVSS 4.0) |
| Status | A new CVE record, published by VulDB on 24 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 25 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 Netis WF2409E router. The record lists firmware up to and including 20261026 as affected. Those whose management interface is reachable from the internet face the greatest immediate risk. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run a Netis WF2409E router? | Nothing to do for this CVE. | Establish whether its management interface is reachable from untrusted networks. |
| Is the router's management interface reachable from the internet or from untrusted network segments? | Risk is lower; restrict access to trusted hosts only and watch for a firmware update. | Block external access immediately — an exploit is publicly available. |
| Is firmware version 20261026 or earlier installed? | No unaffected version is recorded; no source confirms a fix. Treat as affected. | No patch is recorded. Restrict access and monitor for a fix. |

## What it is

An unauthenticated attacker who can reach the router's web management interface can manipulate authentication-related parameters, bypassing the normal login requirement. The record says an exploit is publicly available and may already be in use.

## Things people will get wrong

- A firewall in front of the router makes the management interface safe. The record says the attack can be initiated remotely. Any network path to the management port is sufficient. Confirm the interface is not reachable from outside your network.
- There must be a fixed firmware because the affected range lists an end date. The record lists 20261026 as the last known affected version and names no unaffected release. The vendor did not respond to disclosure. No source names a fixed version.

## How we would triage it

This is our judgement.

## Step 1: Find out whether you run a Netis WF2409E

- Check your network asset list or the router's admin interface for the model name. The record says all firmware up to and including 20261026 is affected.
- If the router was supplied by an ISP, ask them to confirm the model and firmware version.

## Step 2: Check and restrict management interface access

- Log in to the router and look for a remote management or WAN-access setting. Disable it if it is on.
- Restrict management access to your local network or specific trusted IP addresses only.

## Step 3: Reduce exposure while no patch exists

- The record names no fixed firmware version and the vendor did not respond to disclosure. Configure the router or a device in front of it to block access to the management port from untrusted sources.
- If no patch appears and the device is internet-facing, consider replacing it.

## Step 4: Watch for a firmware update from Netis

- No source currently names a fixed version. Check the Netis support pages for the WF2409E for a release dated after 20261026.
- Apply any update promptly once one appears and verify the management interface remains restricted.

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 are following up on CVE-2026-136136, a vulnerability affecting Netis WF2409E routers on firmware 20261026 and earlier. The flaw allows an unauthenticated attacker to bypass authentication through the router's web management interface. The record scores this 10 out of 10 under CVSS 4.0, an exploit is publicly available, and no fixed firmware version has been recorded. Could you please confirm whether we run this device, which firmware version is installed, and whether the management interface is reachable from outside our network? We would appreciate written confirmation of these details and the steps taken as soon as possible.*

## The weakness behind it

The record classes this as CWE-287.

## 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 |
|---|---|---|
| Modify Authentication Process (T1556): Changing how the system checks logins so that a wrong or empty password is accepted. | Credential Access: stealing logins | CWE-287 (Improper Authentication) on a router's authentication endpoint would likely involve manipulating the authentication process to gain access without valid credentials. |

| | | |
|---|---|---|
| Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access. | Persistence: staying in | The affected parameters include password-setting fields; an attacker gaining access would likely be able to modify the device's admin credentials to maintain control. |

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 identified in Netis WF2409E up to 20261026. Affected by this issue is some unknown functionality of the file /cgi-bin/skk_set.cgi of the component CGI Interface. The manipulation of the argument app/password/new_pwd_confirm/passwd_set/mode_name/wl_link leads to improper authentication. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Netis WF2409E the record lists as affected:

- 20261026

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-2026-136136
```

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-2026-136136
```

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

- No fixed firmware version is recorded; the vendor did not respond to disclosure and no patch timeline is known.
- The record does not say whether the flaw affects only the web management interface or other interfaces on the device.
- The record does not describe what an attacker can do beyond bypassing authentication — for example, whether this gives full administrative access.
- No information is available on whether Netis intends to issue a fix or whether the device is approaching end of support.
- 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 25 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-2026-136136**: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P`
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. |
| Attack requirements | None | Works against a default deployment. |
| Privileges required | None | No account is needed. |
| User interaction | None | No one has to do anything. |
| Vulnerable system: confidentiality | High | Total loss of confidentiality. |
| Vulnerable system: integrity | High | Total loss of integrity. |
| Vulnerable system: availability | High | Total loss of availability. |
| Subsequent systems: confidentiality | High | Total loss of confidentiality. |
| Subsequent systems: integrity | High | Total loss of integrity. |
| Subsequent systems: availability | High | Total loss of availability. |

## Appendix 2. Timeline

| Date | Event |
|---|---|
| 24 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 |
|---|---|---|
| Netis WF2409E with management interface exposed to the internet, firmware ≤ 20261026 | Medium | Immediately — block external access today |

| | | |
|---|---|---|
| Netis WF2409E on an internal network, management interface not internet-facing, firmware ≤ 20261026 | Medium | This week — restrict access and watch for a patch |
| Netis WF2409E managed by an ISP or third party with no direct access | Medium | This week — contact the manager and ask about exposure and a fix |
| No Netis WF2409E in the estate | None | None for this CVE |

## Appendix 4. Definition of done

- Every Netis WF2409E 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-2026-136136: https://www.cve.org/CVERecord?id=CVE-2026-136136
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442884
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442884/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-136136