contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Panabit Smart Application Gateway: new CVE

CVE-2026-135792 · record published 24 November 2026

Analysis Report

CVE-2026-135792 in Panabit Smart Application Gateway, a new record scored 10 and not on CISA's exploited list when we read it. What it is, who is affected, and what to check first.

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/panabit-smart-application-gateway-cve-2026-135792

The bottom line

> *Check whether you run Panabit Smart Application Gateway. If you do, read the vendor's page for the fixed version and update. Nothing public says yet that anyone is using this flaw.*

At a glance

Fact	Detail
Product	Panabit Smart Application Gateway (CVE-2026-135792)
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	Organisations running Panabit Smart Application Gateway on version TANGr7p10, especially where the device's web interface is reachable from outside the managed network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Panabit Smart Application Gateway?	Nothing to do for this CVE.	Check whether the firmware version is TANGr7p10 (next question).
Is the firmware version TANGr7p10?	The record names only TANGr7p10 as affected; monitor for further disclosure.	Check whether the web interface is reachable from any untrusted network (next question).
Is the device's web interface reachable from any untrusted network?	Risk is reduced; contact the vendor for a patched version.	Restrict that access immediately, then seek a patch from the vendor.

What it is

An attacker who can reach the email authentication page can pass a crafted Username value that causes the device to run operating-system commands. The record says the attack can be launched remotely and that a working exploit is public.

Why it matters

Our reading is that the combination of a remote network path, OS command injection (CWE-78), and a maximum score of 10 on CVSS 4.0 makes this gateway a credible entry point to anything behind it. A gateway that runs attacker-chosen OS commands can be used to redirect or inspect traffic, alter filtering rules, or move to internal hosts. The exploit is public, the vendor did not reply to advance notice, and the record names no fixed version, so network isolation is the only mitigation available at present.

Things people will get wrong

- No CISA listing means this can wait. The record was published on 24 November 2026 and may not yet have been reviewed for the known-exploited catalogue. The exploit is already public and no vendor patch exists.
- A score of 10 must reflect only a narrow or unusual configuration. The record names TANGr7p10 without stating a narrower condition. A high score reflects severity, not rarity of the configuration needed.

How we would triage it

This is our judgement.

Step 1: Find which firmware version each device runs

- Log in to each Panabit gateway's management console and record the firmware version shown. The record names TANGr7p10 as the affected version.
- If you manage more than one Panabit device, check each one separately — the record does not limit the finding to a particular deployment type.

Step 2: Restrict access to the web interface

- Block untrusted hosts from reaching the management port and the email auth code sender using firewall rules or access-control lists on upstream equipment.
- No workaround is documented in the sources; network isolation is the only measure available until the vendor releases a patched version.

Step 3: Contact the vendor and await a patched release

- The record says the vendor did not respond to advance disclosure. Contact Panabit directly to ask for a patched firmware version and a timeline.
- The record names no fixed version. Do not apply any firmware release as a fix unless the vendor explicitly confirms it addresses CVE-2026-135792.

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 writing about CVE-2026-135792, a maximum-severity OS command-injection flaw in the Panabit Smart Application Gateway, version TANGr7p10. A working exploit is publicly available and the vendor has not released a patch. Please check whether we run any Panabit gateway, confirm the firmware version on each one, and tell us whether the management interface or email authentication page is reachable from any untrusted network. If it is reachable, please restrict that access as soon as possible. We also need to know when a patched firmware version will be available from the vendor. Please send us written confirmation of the version installed on each device and the access restrictions now in place, by 1 December 2026.*

The weakness behind it

The record classes this as CWE-78 and CWE-77.

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 vulnerable endpoint is a web CGI on a network gateway reachable remotely; exploiting the injection flaw would likely be the initial access method for an attacker over the network.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-78 OS command injection would typically result in commands running via a shell interpreter on the host OS, as the weakness description implies.
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	A gateway with OS command access would likely be used to reach hosts on the internal network it filters, making lateral movement the probable next step.

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 has been found in Panabit Smart Application Gateway TANGr7p10. This issue affects the function send_email_authcode of the file user.cgi of the component Email Auth Code Sender. Such manipulation of the argument Username leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Panabit Smart Application Gateway the record lists as affected:

- TANGr7p10

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-2026-135792
```

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-2026-135792
```

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 version is named in the record, and no vendor advisory was available when this was written.
- The record does not state whether reaching the email auth code sender requires a prior login, which affects how widely the attack surface is exposed.
- The record does not describe how much system access a successful exploit would yield on this device.
- The vendor did not respond to advance disclosure; it is not known whether a patch is planned or on what timeline.
- 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 "Does this apply to you?", "What it is", "Why it matters", "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-2026-135792: 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
TANGr7p10 reachable from an internal segment containing untrusted devices	Medium	This week — restrict access and contact the vendor

TANGr7p10 behind a firewall that blocks all untrusted access to its web interface	Low	Next patch cycle — monitor the vendor for a fix
Panabit gateway running a version other than TANGr7p10	Low	Monitor — the record names only TANGr7p10

Appendix 4. Definition of done

- Every Panabit Smart Application Gateway 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-2026-135792: https://www.cve.org/CVERecord?id=CVE-2026-135792
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442755
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442755/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-135792