3 October 2026 · Teemu Tapanila and Juha Jussila · 6 min read

Two vulnerabilities in Comelit’s 1456B door-entry gateway

ADVISORY SUMMARY

CVE-2026-80276 7.5 High

Unauthenticated management interface discloses the remote configuration password

CWE-306

CVE-2026-80275 8.8 High

Any logged-in user can overwrite the installer (administrator) password

CWE-425 • Vendor declined to fix

PRODUCT	PATCH	COORDINATED BY
Comelit 1456B Multi-User Gateway	None available	NCSC-FI

Last updated 3 October 2026

01

Summary

We found two vulnerabilities in the Comelit 1456B Multi-User Gateway (https://pro.comelitgroup.com/en-us/product/1456B), the central unit of Comelit’s VIP door-entry system. It’s used in apartment buildings and offices to run the intercom, the door locks and residents’ access. The vulnerabilities are tracked as CVE-2026-80276 (https://www.cve.org/CVERecord?id=CVE-2026-80276) and CVE-2026-80275 (https://www.cve.org/CVERecord?id=CVE-2026-80275), and the CVE records were published on the 1st of October, 2026.

Either vulnerability is enough to take full control of the gateway system. The first vulnerability only needs network access to the device. The second vulnerability needs low-privileged authentication. There is no patch, and Comelit has said it won't fix CVE-2026-80275.

The most important thing to check is **whether your gateway can be reached from the internet**. If it can, anyone can exploit the first vulnerability without a password. Remote access should go through Comelit's cloud service, MyComelit, or through a VPN. It should never go through a port forwarded straight to the device.

02

What is a Comelit VIP system and what does the gateway component do?

A door-entry system is the panel at the street door, the handset or screen in each apartment, and the wiring between them. Most newer systems are also connected to the internet so residents can answer the door from their phone. The Comelit VIP system is a collection of components making up the entire door-entry system.

The 1456B gateway component connects all of this to the building's network and external networks such as the internet. Installers configure the gateway with Comelit's VIP Manager software. This configuration is where you set which call button rings which apartment, and what entry codes and key fobs open which doors. Whoever controls the gateway decides who can get into the building.

03

The vulnerabilities

Neither attack needs physical access to the building or any help from someone inside the building, if the system is reachable from the public internet. In cases which the system is only accessible locally, a physical access to the network cabling enables system exploitation.

We are not publishing the technical exploit details or any step-by-step guides. Only research general results to help with system protection.

CVE-2026-80276: management interface without a login

The gateway has a management interface meant for administrators, and it doesn't ask for a password. Anyone who can reach it over the network can read the device's configuration. This configuration data includes the remote configuration password in plain text, and with that password an attacker has full access to the device.

CVE-2026-80275: any user can change the installer password

The gateway has several user levels. The installer account is the highest. The function that changes the installer's password checks that you're logged in, but not which account you're logged in with. So any user, including the lowest-level one, can set a new installer password, take over the installer account and lock the real installer out.

Comelit told us this is how the device is meant to work and declined to fix it. We disagree. If the lowest-level account can take over the administrator account, the separate privilege levels and accounts don't protect anything.

04

What an attacker can do

With installer access, an attacker can do anything your installer can. In practice that means they can:

- delete apartments from the system, or revoke residents' codes, key fobs and app access so they can't get in
- send call buttons to the wrong apartment, or change entry codes, door permissions and schedules, for example so a door unlocks itself at night
- add their own code, key fob or app user. Nothing else changes, so it's unlikely anyone would notice
- open doors and gates remotely, if the system is set up for remote door release
- use the cameras and microphones in the entry panels, and in some buildings the ones in the apartments

In some buildings the door-entry system is also connected to emergency exits or lift control.

05

Comelit's response

Comelit acknowledged our report of CVE-2026-80276 on 30 March 2026 and gave it the tracking ID VMP-41. We haven't heard from them about it since. For CVE-2026-80275, they told us the behaviour is intended and won't be fixed.

Comelit's installation guidance says the gateway should sit behind a firewall with only specific ports open. That does help against CVE-2026-80276: if nobody outside can reach the device, nobody outside can attack it. We still don't think a firewall solves this. Installers don't always follow the guidance, and one wrong port-forward is enough to expose the device. A firewall also does nothing about people who

are already on the building's network. In a building with many tenants that could be a neighbour on a shared connection, a guest on the Wi-Fi or a compromised smart device.

06

If you own or manage a building

You don't need to be technical to deal with this. Ask your installer or maintenance company these questions:

1. Do we have a Comelit door-entry system with a 1456B gateway?
2. Can the gateway be reached from the internet? If any port is forwarded to it, ask them to remove the forward.
3. How does remote access work? It should go through MyComelit or a VPN.
4. If the gateway has ever been reachable from the internet, have all three of its passwords been changed since?
5. Is the door-entry system on its own network, separate from office computers, guest Wi-Fi and residents' connections?

If the answers are vague, or the whole answer is "it's behind a firewall", keep asking. A competent installer can tell you whether the gateway is exposed and fix it quickly if it is.

07

If you install or maintain these systems

- Make sure nothing forwards inbound traffic to the gateway, and test it from outside the building's network. A firewall configuration that looks right isn't proof.
- Put the door-entry system on its own VLAN, away from office machines, guest Wi-Fi and residents' connections. That limits who on the local network can reach the management interface, which a firewall at the edge doesn't.
- Use MyComelit for remote access. The gateway connects out to the service, so no inbound ports need to be open.
- If you need direct remote access, use a VPN into the building network and reach the gateway from inside.
- Change all three passwords. If the gateway has been reachable from the internet, assume the old ones are known.

- Because of CVE-2026-80275, treat every account on the gateway as if it had administrator rights, and only give accounts to people you'd trust with full control.
- When you're done, check again from outside that the management interface doesn't respond.

08

Timeline

CVE-2026-80276

DATE	EVENT
2026-03-30	Comelit acknowledged the report (tracking ID VMP-41). No timeline for a fix.
2026-06-06	Reported to NCSC-FI, asking them to coordinate with Comelit
2026-10-01	CVE record published

CVE-2026-80275

DATE	EVENT
2026-03-30	Comelit acknowledged the report (tracking ID VMP-40)
2026-04-10	Comelit declined to fix it, saying the behaviour is intended. We disputed this as a breach of privilege separation.
2026-06-06	Reported to NCSC-FI, asking them to coordinate with Comelit
2026-10-01	CVE record published

09

Credits

Both vulnerabilities were found by Teemu Tapanila and Juha Jussila. NCSC-FI, the National Cyber Security Centre Finland, coordinated the disclosure.

Since there's no fix, we've left out the technical details that would make these vulnerabilities easier to exploit. If you think you have an affected system, start by making sure it can't be reached from the

internet.