Moxa AIG-302 ThingsPro Edge: two flaws could expose secrets and key material



CISA published an advisory on two vulnerabilities in Moxa AIG-302 ThingsPro Edge firmware 1.4.0 and earlier, rated CVSS v3 8.1. Exploitation could disclose sensitive information. Moxa has provided a fix.

- Affected: Moxa AIG-302 ThingsPro Edge firmware version 1.4.0 and earlier.
- Two CVEs: CVE-2026-109812 and CVE-2026-109813, covering missing authorization and use of a hard-coded cryptographic key.
- CVSS v3 score is 8.1; the impact is disclosure of sensitive information.
- CVE-2026-109812 involves the internal API /api/v1/secrets/ and requires a privileged, authenticated attacker with adjacent network access.
- Moxa has provided a fix; the sectors listed are critical manufacturing, energy, and water and

> wastewater.

CISA has published an industrial control systems advisory covering two vulnerabilities in the firmware of the Moxa AIG-302 ThingsPro Edge. All versions up to and including 1.4.0 are listed as affected. The advisory gives a CVSS v3 score of 8.1 and says successful exploitation could let an attacker obtain and disclose sensitive information.

What the advisory says

The two issues are tracked as CVE-2026-109812 and CVE-2026-109813. The weaknesses are described as **missing authorization** and **use of a hard-coded cryptographic key**.

For CVE-2026-109812, the flaw sits in the internal API /api/v1/secrets/. A privileged, authenticated attacker with adjacent network access could use it to reach sensitive information, including cryptographic key material. The excerpt we reviewed does not give the details of CVE-2026-109813.

Moxa is based in Taiwan and its products are deployed worldwide. CISA lists critical manufacturing, energy, and water and wastewater systems among the relevant sectors. The advisory notes that Moxa has provided a fix.

What it means for operators

The stated conditions, privileged access and adjacent network position, narrow the likely attack paths. They do not remove the risk where management or operational networks are poorly segmented. Exposed key material can also have effects beyond the device itself, so operators should treat this as a credential-hygiene matter as well as a patching one.

Organizations should first confirm whether any of these devices are in service, then follow the vendor's remediation guidance.

What to do now

1. Inventory OT and edge environments for Moxa AIG-302 ThingsPro Edge devices and record firmware versions.
2. Apply the fix provided by Moxa to any device running firmware 1.4.0 or earlier, following change control and testing procedures.
3. Restrict adjacent network access to these devices through segmentation and limit which accounts hold privileged access.
4. Review whether keys or secrets stored on or used by affected devices need to be rotated once patched.
5. Record the exposure and remediation status in your OT risk register and report it under your internal OT security governance.