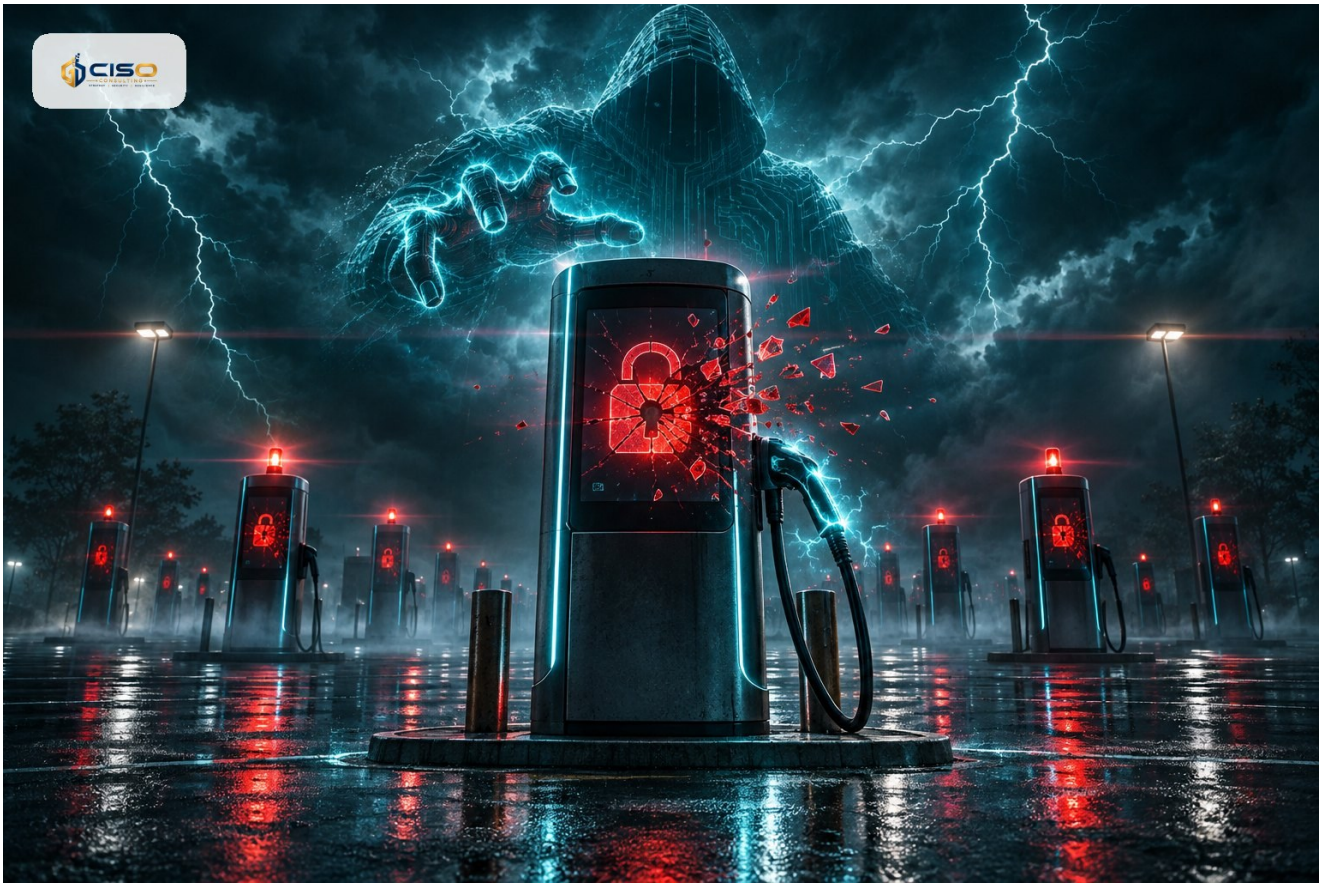
CISA flags critical flaws in Monta monta.app EV charging platform



CISA published an ICS advisory on Monta monta.app covering four vulnerabilities (CVSS v3 9.4) that could give attackers administrative control of charging stations or disrupt charging services. All versions are affected.

- Four CVEs affect all versions of Monta monta.app: CVE-2026-95102, CVE-2026-97363, CVE-2026-97212 and CVE-2026-93474.
- The CVSS v3 score is 9.4.
- Weakness types: missing authentication for a critical function, excessive authentication attempts, insufficient session expiration and insufficiently protected credentials.
- CVE-2026-95102: WebSocket endpoints lack authentication, allowing attackers to impersonate charging stations.

> - Impact: unauthorized administrative control of stations or denial of service. Sectors listed: Energy and Transportation Systems.

CISA has released an industrial control systems advisory on monta.app, the charging-management product from Monta, a company headquartered in the Netherlands. The advisory covers four vulnerabilities and rates them 9.4 on the CVSS v3 scale. The source lists all versions as affected.

What the advisory describes

The weaknesses are missing authentication for a critical function, improper restriction of excessive authentication attempts, insufficient session expiration and insufficiently protected credentials. They are tracked as CVE-2026-95102, CVE-2026-97363, CVE-2026-97212 and CVE-2026-93474.

For CVE-2026-95102, WebSocket endpoints do not properly authenticate callers. An attacker could impersonate a charging station, reach sensitive data or perform unauthorized actions, and because no authentication is needed this may lead to privilege escalation across the wider system. The source excerpt does not detail the other three CVEs.

CISA states that successful exploitation could give attackers unauthorized administrative control of vulnerable charging stations, or allow them to disrupt charging services through denial of service. The advisory lists the Energy and Transportation Systems sectors and notes worldwide deployment.

Why it matters locally

Organizations in the Kingdom that operate or host EV charging infrastructure, or that rely on a provider using this platform, should confirm whether monta.app is part of their environment. The excerpt does not mention a patch or fix, so teams should consult the full CISA advisory and the vendor for current mitigation guidance.

What to do now

1. Check whether monta.app is used in your charging infrastructure or by your charging service providers.
2. Read the full CISA advisory and contact Monta or your provider for fixes and mitigation guidance.
3. Restrict network exposure of charging-management and WebSocket endpoints to trusted sources only.
4. Monitor for unexpected station registrations, administrative actions and repeated authentication attempts.
5. Review session lifetimes and credential storage for charging-management accounts.
6. Add the exposure to your OT risk register and align the response with NCA OTCC controls.