

Monta-Ladeplattform: Ladesäulen übernehmbar

Stand 17.10.2026 10:02 · Sendung: - · · Belegstärke: **bestätigt** · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 48 % ■ Wahrscheinlich 20 % ■ Nicht bekannt 32 %

Die technischen Kernfakten und Gegenmaßnahmen sind durch das CISA-Advisory gut belegt, ein Angriff ist nicht bekannt, und zur Zahl der Ladepunkte ohne Authentifizierung und zum Stand der Umstellung im Feld gibt es keine öffentlichen Angaben; dazu kommt die Unstimmigkeit beim Firmensitz (CISA: Niederlande, Fachpresse: Dänemark).

1. Was ist passiert, und warum?

WISSEN

- CISA hat am 01.10.2026 das Advisory ICSA-26-274-02 zu Monta monta.app veröffentlicht (Revision 1). Betroffen sind alle Versionen, Sektoren Energy und Transportation Systems, Einsatz weltweit. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- CVE-2026-95102 (CWE-306): WebSocket-Endpunkte ohne Authentifizierung, darüber können sich Angreifer als Ladestation ausgeben. CVSS v3.1 9.4, v4 9.3. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- CVE-2026-97363 (CWE-307): keine Begrenzung der Anmeldeversuche, ermöglicht Brute Force oder Denial-of-Service. CVSS v3.1 7.5, v4 8.7. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- CVE-2026-97212 (CWE-613): unzureichendes Session-Management. Das Backend ordnet Sitzungen über die Stations-Kennung zu und lässt mehrere Endpunkte mit derselben Sitzungskennung zu, möglich sind Identitätsmissbrauch und Überlastung des Backends. CVSS v3.1 7.3, v4 6.9. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- CVE-2026-93474 (CWE-522): Authentifizierungs-Kennungen der Ladestationen sind über webbasierte Kartendienste öffentlich einsehbar. CVSS v3.1 6.5, v4 6.9. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- Gemeldet hat die Schwachstellen ein anonymer Researcher an CISA. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- Laut Monta-Stellungnahme im Advisory arbeitet das Unternehmen daran, authentifizierte Verbindungen zu verbreiten und Zugänge ohne Authentifizierung schrittweise abzuschalten. Solche Zugänge existieren also derzeit noch. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]
- Dieselben vier Schwachstellenklassen (CWE-306, -307, -613, -522) mit identischen CVSS-Werten hat CISA 2026 auch für ev.energy (26.02.), Everon (03.03.) und EVOKE (25.06.) veröffentlicht, gemeldet jeweils von Khaled Sarieddine und Mohammad Ali Sayed. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-08>]
- Das EVOKE-Advisory gehört zur selben Reihe. (100 %)
[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-02>]
- Forscher der Concordia University und des Hydro-Québec Research Institute fanden 2024 sechs Zero-Day-Schwachstellen in 16 live betriebenen OCPP-Backends, Ursachen waren unter anderem schwache Authentifizierung und mangelhaftes Session-Management. (100 %)
[<https://cyberinsider.com/security-flaws-uncovered-in-ev-charging-infrastructure-ocpp-backends/>]

- Als Firmensitz nennt CISA „Netherlands“, die Fachpresse beschreibt Monta als dänisches Unternehmen (Kopenhagen). (100 %)

[<https://www.electrive.net/2026/09/25/mvv-energie-buendelt-6-600-ladepunkte-auf-monta-plattform/>]

NICHT BEKANNT

- Wer der anonyme Researcher ist und ob er dieselbe Methode wie bei den früheren Lade-Advisories genutzt hat
- Seit wann die Schwachstellen bestehen und wann Monta informiert wurde
- Wie viele Ladepunkte zum Zeitpunkt der Meldung ohne Authentifizierung verbunden waren
- Warum CISA als Sitz die Niederlande angibt (Fehler oder Bezug auf eine Tochtergesellschaft)

WAHRSCHEINLICH (Einschätzung)

- Die Ursache ist ein Branchenmuster aus Abwärtskompatibilität: Damit ältere OCPP-1.6-Ladesäulen weiterlaufen, nehmen Plattformen Verbindungen ohne starke Anmeldung an. (78 %) – Vier Backends mit identischem Schwachstellenbild, Monta schaltet Zugänge ohne Authentifizierung nur schrittweise ab, EVOKE nennt ausdrücklich nicht mehr unterstützte Altgeräte.
- Die Meldung beruht auf derselben Testmethode wie die früheren Lade-Advisories. (55 %) – Gleiche CWE-Struktur, gleiche CVSS-Werte, fast gleicher Wortlaut und dieselbe Sitzangabe „Netherlands“ wie bei Everon sprechen dafür. Der Researcher ist aber anonym, die Verbindung ist nicht belegt (A 55 %, B 60 %).

2. Was ist die Auswirkung?

WISSEN

- Laut CISA könnten Angreifer unbefugt administrative Kontrolle über Ladestationen erlangen oder Ladedienste per Denial-of-Service stören. (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- CISA ist keine öffentliche Ausnutzung bekannt (Stand 01.10.2026). (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- Laut Fachpresse wurde kein öffentlicher Exploit-Code veröffentlicht. (100 %)

[<https://securityonline.info/monta-ev-charging-vulnerabilities/>]

- Das BSI hält es bei Angriffen auf Ladeinfrastruktur allgemein für möglich, dass ganze Regionen zeitweise nicht laden können, und schließt negative Folgen für die Netzstabilität nicht aus (nicht auf Monta bezogen). (100 %)

[<https://www.zfk.de/mobilitaet/e-mobilitaet/bund-warnt-ladesaeulen-anfaellig-fuer-cyberangriffe>]

- Laut Bericht über den ersten BSI-Bericht zur Ladeinfrastruktur können Angriffe zu Schäden an Fahrzeugen oder Ladeinfrastruktur, zu Mobilitätseinschränkungen und bis zu Ausfällen vorgelagerter Netze führen (allgemein, nicht auf Monta bezogen). (100 %)

[<https://ecomento.de/2026/05/08/bsi-veroeffentlicht-bericht-zur-it-sicherheit-der-oeffentlichen-ladeinfrastruktur/>]

NICHT BEKANNT

- Ob die Lücken vor der Veröffentlichung ausgenutzt wurden
- Ob Abrechnungs- oder Kundendaten betroffen sein könnten (das Advisory nennt das nicht ausdrücklich)
- Ob ein Angreifer über die Lücken echte Ladesäulen steuern kann oder nur das Backend täuscht

WAHRSCHEINLICH (Einschätzung)

- Wer sich als Ladesäule ausgibt, kann echte Säulen vom Backend verdrängen und falsche Daten (Status, Zählerstände) einspeisen. (70 %) – Die Advisories zu Everon und ev.energy beschreiben ausdrücklich Verdrängung legitimer Stationen und Datenmanipulation, bei Monta beschreibt CISA dieselbe Klasse (nur von B bewertet).
- Realistisch sind lokale bis regionale Störungen: Ladepunkte erscheinen offline, Ladevorgänge scheitern oder Abrechnungen stimmen nicht. Eine flächige Gefahr für das Stromnetz ist daraus nicht abzuleiten. (60 %) – Die Lücken betreffen die Kommunikation Säule zu Backend. Bei über 330.000 verwalteten Ladepunkten wäre eine länderübergreifende Störung denkbar, und das BSI schließt Netzfolgen bei großflächigen Angriffen nicht aus. Netzrelevanz ist für Monta aber nicht

belegt.

- Ein Angreifer kann über diese Lücken echte Ladevorgänge direkt starten, stoppen oder die Ladeleistung vorgeben (widersprüchlich: A 50 % / B 35 %). (35 %) – CISA spricht von administrativer Kontrolle, nennt aber keine konkreten Befehle. In OCPP schickt das Backend Steuerbefehle an die Säule, die Lücke erlaubt vor allem, sich gegenüber dem Backend als Säule auszugeben. B ist hier besser begründet, deshalb der niedrigere Wert.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

- Monta hat laut eigener Angabe auf der WebSocket-Ebene Rate Limiting und automatische Drosselung missbräuchlicher Verbindungen eingeführt. (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- Monta unterstützt OCPP 1.6 Security Profile 2 (HTTP Basic Auth mit TLS) und fordert die Betreiber auf, es zu aktivieren. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- Monta will Zugänge ohne Authentifizierung schrittweise abschalten, eine neue authentifizierte Verbindung ersetzt laut Monta die bestehende Sitzung derselben Station. (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- Zum Vergleich: EVOKE migriert Ladegeräte gemeinsam mit den OEMs auf Security Profile 2 oder 3 und akzeptiert bei Altgeräten nur noch registrierte IDs, eine Lebenszyklusrichtlinie für Altgeräte ist erst in Arbeit. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-02>]

NICHT BEKANNT

- Bis wann Monta Zugänge ohne Authentifizierung ganz abschaltet
- Wie viele Ladesäulen-Modelle im Feld Security Profile 2 per Firmware überhaupt unterstützen
- Ob Monta die Weitergabe der Stations-IDs an Kartendienste eingeschränkt hat

WAHRSCHEINLICH (Einschätzung)

- Auf der Plattform selbst sind die Lücken in Tagen entschärft, die Umstellung aller Ladepunkte im Feld dauert bei gemischten Beständen Wochen bis Monate. (65 %) – Rate Limiting ist zentral umsetzbar und schon aktiv. Security Profile 2 braucht an jeder Säule eigene Zugangsdaten, teils neue Firmware und die Mitarbeit der Hardware-Hersteller, wie das EVOKE-Advisory zeigt. A und B übereinstimmend.

- Ein Teil der älteren Ladesäulen kann Security Profile 2 nicht und muss ersetzt oder gesondert abgeschirmt werden (widersprüchlich: A 45 % / B 55 %). (45 %) – EVOKE spricht ausdrücklich von nicht mehr unterstützten Altgeräten, Monta ist mit über 900 Modellen kompatibel. Belegte Zahlen zur Unterstützung fehlen, deshalb der niedrigere Wert.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

- Das Advisory nennt als mögliche Folgen Kontrollübernahme und Denial-of-Service, keine physischen Schäden, eine Ausnutzung ist nicht bekannt. (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

- Das BSI hält bei Angriffen auf Ladeinfrastruktur allgemein Schäden an Fahrzeugen und Infrastruktur für möglich (nicht auf Monta bezogen). (100 %)

[<https://www.zfk.de/mobilitaet/e-mobilitaet/bund-warnt-ladesaeulen-anfaellig-fuer-cyberangriffe>]

- Der BSI-Bericht zur Ladeinfrastruktur nennt allgemein mögliche Schäden an Fahrzeugen oder Ladeinfrastruktur durch Angriffe. (100 %)

[<https://ecomento.de/2026/05/08/bsi-veroeffentlicht-bericht-zur-it-sicherheit-der-oeffentlichen-ladeinfrastruktur/>]

NICHT BEKANNT

- Ob über diese Schwachstellen Ladeparameter so verändert werden könnten, dass Hardware Schaden nimmt
- Ob über das Backend Firmware-Updates an Ladesäulen ausgelöst werden könnten
- Ob einzelne Säulen-Modelle auf manipulierte Backend-Daten mit Fehlfunktion reagieren

WAHRSCHEINLICH (Einschätzung)

- Hardware wird durch diese Schwachstellen nicht dauerhaft beschädigt, betroffen sind Steuerung, Verfügbarkeit und Abrechnung. (75 %) – Die Lücken liegen im Backend und betreffen Anmeldung und Sitzungen, Ladesäule und Fahrzeug haben eigene Schutzfunktionen. Das BSI nennt Hardwareschäden allgemein als möglich, ohne Herstellerangaben lässt sich das nicht ganz ausschließen. A und B übereinstimmend.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Laut electrive (25.09.2026) verwaltet Monta mehr als 330.000 Ladepunkte, ist direkt in zwölf europäischen Märkten aktiv und mit über 900 Ladesäulen-Modellen von 274 Herstellern kompatibel. (100 %)

[<https://www.electrive.net/2026/09/25/mvv-energie-buendelt-6-600-ladepunkte-auf-monta-plattform/>]

- MVV Energie stellt rund 6.600 Ladepunkte in Deutschland auf die Monta-Plattform um, davon gut 500 öffentlich und etwa 6.100 gewerblich. (100 %)

[<https://www.electrive.net/2026/09/25/mvv-energie-buendelt-6-600-ladepunkte-auf-monta-plattform/>]

- Team Emobility migriert über 1.800 Ladepunkte auf Monta. (100 %)

[<https://www.electrive.net/2026/01/16/team-emobility-stellt-auf-monta-plattform-um/>]

- Eliso (Stuttgart) stattet Ladepunkte, darunter 828 Punkte im Deutschlandnetz, mit Monta-Software für Bezahlung und Abrechnung aus. (100 %)

[<https://www.electrive.net/2024/06/11/eliso-setzt-auf-abrechnungsloesung-von-monta/>]

- Mit Monta sind 2026 vier Lade-Backends mit demselben Schwachstellenmuster in CISA-Advisories erschienen. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-02>]

- 2024 fanden Forscher der Concordia University und des Hydro-Québec Research Institute sechs Zero-Days in 16 live betriebenen OCPP-Backends weltweit (Pressebericht). (100 %)

[<https://cyberinsider.com/security-flaws-uncovered-in-ev-charging-infrastructure-ocpp-backends/>]

- Shodan (aggregiert): Monta-Plattform für rund 6.600 Ladepunkte von MVV Energie: ca. 0 öffentlich erreichbare Systeme in Deutschland (100 %)

- Shodan (aggregiert): Monta-Plattform für über 1.800 Ladepunkte von Team Emobility: ca. 0 öffentlich erreichbare Systeme in Deutschland (100 %)

- Shodan (aggregiert): Monta-Software für Bezahlung und Abrechnung bei Eliso: ca. 0 öffentlich erreichbare Systeme in Deutschland (100 %)

- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 143086 gesamt (DNP3 33392, OMRON FINS 23267, ProConOS 16506, EtherNet/IP 15855, Siemens S7 8211, OPC UA 5676) (100 %)

NICHT BEKANNT

- Welcher Anteil der Monta-Ladepunkte ohne Authentifizierung angebunden ist

- Wie viele Stadtwerke in DACH Monta einsetzen (es gibt keine vollständige Liste)

- Wie viele weitere Lade-Backends dasselbe Muster haben, aber noch nicht geprüft oder gemeldet sind

- Woher die früher genannte Zahl „über 300.000“ stammt

WAHRSCHEINLICH (Einschätzung)

- Weitere OCPP-Backends haben ähnliche Schwächen, die noch nicht öffentlich gemeldet sind. (70 %) – Vier gleichartige Advisories in acht Monaten, 16 untersuchte Systeme in der Studie von 2024, OCPP 1.6 ohne Security Profile ist weit verbreitet. A und B übereinstimmend.

- Ein relevanter Teil der Monta-Ladepunkte verband sich zum Zeitpunkt des Advisory ohne Security Profile 2. (60 %) – Sonst müsste Monta den Zugang ohne Authentifizierung nicht schrittweise abschalten. Eine Zahl dazu ist nicht veröffentlicht.

6. Kann das wieder passieren?

WISSEN

- Dasselbe Muster aus vier Schwachstellen trat 2026 bei ev.energy, Everon, EVOKE und Monta auf, ev.energy hat laut CISA nicht auf die Koordinationsanfrage reagiert. (100 %)

[<https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-07>]

- Das BSI sieht bei OCPP Nachbesserungsbedarf in der sicheren Implementierung und fordert Security by Design und Security by Default. (100 %)

[<https://www.ingenieur.de/technik/fachbereiche/itk/wie-sicher-sind-oeffentliche-ladesaeulen/>]

- OCPP 1.6 kennt mit Security Profile 2 bereits eine Absicherung per HTTP Basic Auth und TLS, Monta empfiehlt sie den Betreibern. (100 %) [<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>]

NICHT BEKANNT

- Ob es in DACH verbindliche Vorgaben für authentifizierte OCPP-Verbindungen geben wird
- Ob ev.energy die Schwachstellen inzwischen behoben hat

WAHRSCHEINLICH (Einschätzung)

- In den nächsten Monaten erscheinen weitere Advisories zu Lade-Backends mit ähnlichen Schwachstellen. (75 %) – Die Reihe läuft seit Februar 2026 in kurzen Abständen, und Sicherheitsfunktionen in OCPP sind weiterhin optional.
- Ein tatsächlicher Angriff auf eine Ladeplattform in DACH mit spürbarem Ausfall wird öffentlich bekannt. (25 %) – Die Schwachstellen sind verbreitet, belegte Angriffe auf Lade-Backends in DACH sind aber bisher nicht dokumentiert.

Lage

CISA hat am 01.10.2026 das Advisory ICSA-26-274-02 zu allen Versionen der Ladeplattform monta.app veröffentlicht: Vier Schwachstellen in der OCPP-WebSocket-Anbindung, die kritischste mit CVSS 9.4, erlauben es Angreifern, sich gegenüber dem Backend als Ladesäule auszugeben, Sitzungen zu übernehmen oder den Ladebetrieb zu stören. Eine Ausnutzung ist laut CISA nicht bekannt, Monta hat Rate Limiting eingeführt, will Verbindungen ohne Authentifizierung schrittweise abschalten und empfiehlt den Betreibern OCPP 1.6 Security Profile 2 mit TLS. Dasselbe Muster hat CISA 2026 schon bei drei anderen Lade-Backends veröffentlicht, in Deutschland nutzt unter anderem MVV Energie die Plattform für rund 6.600 Ladepunkte.

Angriff	Kein Angriff bekannt. Es handelt sich um ein koordiniertes Schwachstellen-Advisory zu einer Ladeplattform (OCPP-Backend).
Wann / Status	Advisory veröffentlicht am 01.10.2026 · unklar
Täter	Kein Threat Actor bekannt, CISA meldet keine Ausnutzung. – unbekannt
Betreiber / Branche	Monta (Plattform monta.app), Betreiber auf der Plattform sind nicht namentlich als betroffen genannt · E-Mobilität, Ladeinfrastruktur-Software (CPMS), laut CISA Sektoren Energy und Transportation Systems
Anlage / Alter	Cloud-Backend zur Steuerung und Abrechnung von Ladesäulen über OCPP · unbekannt, betroffen sind alle Versionen
Region	weltweit, direkt in zwölf europäischen Märkten aktiv (laut A auch USA); Unstimmigkeit beim Sitz: CISA nennt die Niederlande, Fachpresse beschreibt Monta als dänisches Unternehmen (Kopenhagen)

Eingesetzte Produkte (öffentlich belegt)

- Monta-Plattform für rund 6.600 Ladepunkte von MVV Energie (Monta) – Presse
[<https://www.electrive.net/2026/09/25/mvv-energie-buendelt-6-600-ladepunkte-auf-monta-plattform/>]
- Monta-Plattform für über 1.800 Ladepunkte von Team Emobility (Monta) – Presse
[<https://www.electrive.net/2026/01/16/team-emobility-stellt-auf-monta-plattform-um/>]
- Monta-Software für Bezahlung und Abrechnung bei Eliso (u. a. 828 Ladepunkte im Deutschlandnetz) (Monta) – Presse
[<https://www.electrive.net/2024/06/11/eliso-setzt-auf-abrechnungsloesung-von-monta/>]

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

- Hypothese: Ausnutzung der fehlenden Authentifizierung an den OCPP-WebSocket-Endpunkten in Verbindung mit öffentlich einsehbaren Stations-Kennungen, um sich gegenüber dem Backend als Ladesäule auszugeben. (hoch): Genau diese Kombination beschreibt CISA (CVE-2026-95102 und CVE-2026-93474), Monta bestätigt indirekt, dass Zugänge ohne Authentifizierung noch bestehen. Eine tatsächliche Ausnutzung ist nicht bekannt.
- Hypothese: Störung des Ladebetriebs per Denial-of-Service über massenhafte Verbindungs- oder Anmeldeversuche. (mittel): CISA nennt fehlende Begrenzung der Anmeldeversuche (CVE-2026-97363) und Überlastung des Backends als Folge. Monta hat Rate Limiting inzwischen eingeführt, das senkt die Plausibilität.
- Hypothese: Dauerhafte Angriffsfläche über ältere Ladesäulen, die Security Profile 2 nicht unterstützen und deshalb weiter ohne Authentifizierung verbunden bleiben. (mittel): Monta schaltet Zugänge ohne Authentifizierung nur schrittweise ab, EVOKE nennt ausdrücklich nicht mehr unterstützte Altgeräte. Wie groß dieser Bestand ist, ist nicht belegt.

Zeitleiste

2024 Concordia University und Hydro-Québec Research Institute finden sechs Zero-Days in 16 live betriebenen OCPP-Backends. – [berichtet](#)

11.06.2024 Eliso setzt für Bezahlung und Abrechnung auf Monta-Software. – [berichtet](#)

16.01.2026 Team Emobility stellt über 1.800 Ladepunkte auf Monta um. – [berichtet](#)

26.02.2026 CISA-Advisory zu ev.energy mit demselben Schwachstellenmuster, ev.energy reagiert nicht auf die Koordinationsanfrage. – [bestätigt](#)

03.03.2026 CISA-Advisory zu Everon mit demselben Schwachstellenmuster. – [bestätigt](#)

08.05.2026 Bericht über den ersten BSI-Bericht zur IT-Sicherheit der öffentlichen Ladeinfrastruktur. – [berichtet](#)

25.06.2026 CISA-Advisory zu EVOKE mit demselben Schwachstellenmuster. – [bestätigt](#)

25.09.2026 MVV Energie bündelt rund 6.600 Ladepunkte auf der Monta-Plattform, Monta verwaltet laut electrive über 330.000 Ladepunkte. – [berichtet](#)

01.10.2026 CISA veröffentlicht ICSA-26-274-02 zu Monta monta.app: vier CVEs, CVSS bis 9.4, keine Ausnutzung bekannt; Monta meldet Rate Limiting und schrittweise Abschaltung von Zugängen ohne Authentifizierung. – [bestätigt](#)

Früherer Stand: Erstmeldung (03.10.2026 09:34)

Wissen 30 % · wahrscheinlich 15 % · nicht bekannt 55 %

Die US-Behörde CISA hat am 01.10.2026 ein Advisory zu vier Schwachstellen in allen Versionen der Cloud-Ladeplattform monta.app veröffentlicht, die schwerste mit CVSS 9.4. Laut CISA fehlt an den OCPP-WebSocket-Endpunkten eine ausreichende Authentifizierung, und die Stations-Kennungen sind öffentlich einsehbar. Angreifer könnten sich deshalb als Ladesäule ausgeben, Stationen übernehmen oder den Ladebetrieb per Denial-of-Service stören. Nach heutigem Stand ist das eine veröffentlichte Schwachstelle und kein bekannter Angriff: CISA ist keine Ausnutzung bekannt, Monta hat Rate Limiting eingeführt und empfiehlt den Betreibern OCPP 1.6 Security Profile 2 mit TLS.

Früherer Stand: Nach 24 Stunden (04.10.2026 17:44)

Wissen 49 % · wahrscheinlich 18 % · nicht bekannt 33 %

Die US-Behörde CISA hat am 01.10.2026 vier Schwachstellen in allen Versionen der Ladeplattform monta.app veröffentlicht. Die schwerste hat CVSS 9.4: Die OCPP-WebSocket-Endpunkte haben keine Authentifizierung, und die Stations-Kennungen sind über Kartendienste öffentlich einsehbar. Deshalb könnten Angreifer sich als Ladesäule ausgeben, Stationen administrativ übernehmen oder den Ladebetrieb stören. Laut CISA ist keine

Ausnutzung bekannt. Monta hat Rate Limiting eingeführt und will Verbindungen ohne Authentifizierung schrittweise abschalten. In Deutschland nutzen u. a. MVV Energie (rund 6.600 Ladepunkte), eliso (Deutschlandnetz) und Team Emobility die Plattform.

Früherer Stand: Nach 72 Stunden (06.10.2026 09:55)

Wissen 53 % · wahrscheinlich 18 % · nicht bekannt 29 %

Am 01.10.2026 hat die US-Behörde CISA ein Advisory zu vier Schwachstellen in allen Versionen der Ladeplattform monta.app veröffentlicht. Die schwerste ist CVE-2026-95102 mit CVSS 9.4: An den OCPP-WebSocket-Endpunkten fehlt die Authentifizierung, und die Stations-Kennungen sind über Kartendienste öffentlich einsehbar. Angreifer könnten sich dadurch als Ladesäule ausgeben, die Kontrolle über Stationen übernehmen oder den Ladebetrieb stören. Eine Ausnutzung ist nicht bekannt. Monta hat Rate Limiting eingeführt, empfiehlt den Betreibern OCPP 1.6 Security Profile 2 (TLS + Basic Auth) und will unauthentifizierte Zugänge schrittweise abschalten. Dieselbe Schwachstellenklasse hat CISA 2026 schon bei mehreren weiteren Lade-Backends gemeldet, darunter ev.energy, CloudCharge, EV2GO, Everon, EVOKE und in ähnlicher Form Hydro-Québec. Es ist also ein Branchenproblem und kein Einzelfall.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.