

Sungrow-Cloud: Zugriff auf 250.000 PV-Anlagen

Stand 10.10.2026 12:41 · Sendung: – · · Belegstärke: **bestätigt** · **berichtet** · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 59 % ■ Wahrscheinlich 21 % ■ Nicht bekannt 20 %

Der Kern ist belastbar, denn der Hersteller hat die Lücke bestätigt, der Forscher hat sie selbst veröffentlicht und BSI, ZEIT/dpa und pv magazine berichten übereinstimmend; unsicher bleiben die Reichweite in Anlagen und GW und vor allem die Frage, ob ein Blackout tatsächlich möglich gewesen wäre.

1. Was ist passiert, und warum?

WISSEN

- Marlon Starkloff, Geschäftsführer der Jakkaru GmbH, fand im August 2026 einen Logikfehler in der Anmeldung von iSolarCloud. Darüber gelangte er ohne Passwort in Nutzerkonten, und die Betroffenen bekamen dabei keine Login-Benachrichtigung (berichtet, Forscher-Primärquelle und dpa). (100 %) [<https://jakkaru.de/articles/sungrow-vulnerability-exposes-gigawatts-worldwide>]
- Von dort kamen die Forscher in Verwaltungskonten großer Installationsbetriebe, laut ComputerBase Enpal und 1KOMMA5°, und anschließend in Admin-Konten von Sungrow (berichtet). (100 %) [<https://www.computerbase.de/news/smart-home/250-000-anlagen-in-deutschland-luecke-in-cloud-von-solar-anbieter-haette-zu-blackout-fuehren-koennen.99717/>]
- Die betroffenen Installationsbetriebe erklären, es habe weder Datenabfluss noch Manipulation von Kundenanlagen gegeben (berichtet). (100 %) [<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud>]
- Sungrow bestätigt, dass am 22.08.2026 ein unabhängiger Forscher eine Schwachstelle im Login-Prozess gemeldet hat, die den Zugriff auf Konten ohne die nötige Authentifizierung erlaubte. Ursache war laut Sungrow ein fehlerhaftes Login-Modul (bestätigt, Herstellerangabe gegenüber Medien). (100 %) [<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]
- Sungrow räumt ein, dass das Login-Modul eine Zeit lang eine Umgehung der Authentifizierung zuließ (berichtet). (100 %) [<https://www.hessenschau.de/wirtschaft/solaranlagen-wie-kritisch-war-die-sungrow-sicherheitsluecke-v4,sicherheitsluecke-solarbranche-100.html>]
- Laut Jakkaru betraf der Fehler alle vier regionalen iSolarCloud-Systeme: Europa, China, Australien und International (berichtet, Forscher-Primärquelle). (100 %) [<https://jakkaru.de/de/artikel/sungrow-vulnerability-exposes-gigawatts-worldwide>]
- Jakkaru hat ohne Auftrag als eigenes Forschungsprojekt gehandelt (berichtet). (100 %) [<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]
- Harm van den Brink (DIVD) kommt im ZEIT- und dpa-Bericht als zitierter Experte vor („Das hätte auf jeden Fall für einen Blackout gesorgt“), nicht als Entdecker des Falls von 2026 (berichtet). (100 %) [<https://www.tagesspiegel.de/wirtschaft/dpa-hacker-hatte-hunderttausende-solaranlagen-in-deutschland-lahmlegen-konnen-16137653.html>]
- Früherer Fall 1: Am 27.12.2023 wurde dem BSI gemeldet, dass ein Installateurkonto Firmware-Updates für fremde Geräte auslösen konnte und die Images nicht signiert waren. Sungrow hat das bis zum 21.04.2024 behoben (Forscher-Primärquelle). (100 %) [<https://veganmosfet.codeberg.page/posts/2024-04-21-solarflaresec/>]

- Früherer Fall 2: Über CVE-2025-29756 (DIVD/ENCS) konnten angemeldete Nutzer per MQTT die Telemetriedaten aller Geräte mitlesen. Gemeldet am 28.03.2025, gepatcht am 06.06.2025 (bestätigt). Darauf bezieht sich vermutlich die Angabe „behoben Juni 2025“. (100 %)

[<https://csirt.divd.nl/cases/DIVD-2025-00009>]

NICHT BEKANNT

- Seit wann die Lücke vor dem 22.08.2026 bestand.
- Ob es für den Fall von 2026 eine CVE gibt: Die in einem Bericht genannte CVE-2026-107194 mit CVSS 9,2 ist in keiner CVE-Datenbank zu finden.
- Wie die technische Ursachenanalyse genau aussieht und was die von Sungrow beauftragte Prüfung durch die NCC Group ergeben hat.

WAHRSCHEINLICH (Einschätzung)

- Die Ursache ist ein Authentifizierungsfehler in der Hersteller-Cloud und kein Fehler von Betreibern oder Installateuren. (92 %) – Forscher und Hersteller beschreiben übereinstimmend einen Fehler im Login-Prozess der Plattform.
- Grundsätzlich liegt es an der Architektur: Nutzer-, Installateur- und Admin-Funktionen laufen auf derselben Plattform, deshalb wirkt ein einzelner Login-Fehler bis ganz nach oben. (75 %) – Jakkaru empfiehlt ausdrücklich, Nutzer- und Admin-Plattformen zu trennen, und die beschriebene Eskalation entlang der Konto-Hierarchie stützt das.
- Dass van den Brink in einigen Berichten als Entdecker genannt wird, kommt von seinem Experten-Zitat und einer Verwechslung mit den DIVD-Fällen zu Sungrow (CVE-2025-29756 sowie eine DIVD-Veröffentlichung vom 19.08.2026). (60 %) – Beide Erklärungen sind plausibel und lassen sich nicht voneinander trennen (widersprüchlich: A 60 % / B 70 %).

2. Was ist die Auswirkung?

WISSEN

- Laut ZEIT waren rund 470.000 Anlagen in Europa erreichbar, davon fast 250.000 in Deutschland (berichtet). (widersprüchlich: A 470.000 / B 470.000–500.000 in Europa) (100 %) [<https://www.computerbase.de/news/smart-home/250-000-anlagen-in-deutschland-luecke-in-cloud-von-solar-anbieter-haette-zu-blackout-fuehren-koennen.99717/>]
- Die Spitzenleistung in Deutschland lag bei etwa 7,8 GW (cleanthinking), laut t3n bei knapp 8 GW. Die Angabe von 10 GW ist nicht bestätigt (berichtet). (100 %) [<https://www.cleanthinking.de/?p=1074028>]
- Ein Screenshot vom Europa-Portal zeigte Ende August zeitweise knapp 18 GW Echtzeit-Erzeugung. Das Verbundnetz ist auf einen plötzlichen Ausfall von bis zu 3 GW ausgelegt (berichtet). (100 %) [<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud/>]
- Laut t3n kamen in Europa etwa 18 GW Spitzenleistung zusammen (berichtet). (100 %) [<https://t3n.de/news/super-blackout-deutschland-hacker-8-gigawatt-1766966/>]
- Weltweit ist die Zahl uneinheitlich: dpa nennt rund 2,2 Millionen Anlagen, hessenschau rund 2,5 Millionen Geräte (berichtet, widersprüchlich). (100 %) [<https://www.hessenschau.de/wirtschaft/solaranlagen-wie-kritisch-war-die-sungrow-sicherheitsluecke-v4,sicherheitsluecke-solarbranche-100.html>]
- Laut Jakkaru ließen sich mit Admin-Rechten Anlagen, Wechselrichter und Batteriespeicher auflisten, ändern, starten und stoppen sowie eigene Firmware aufspielen (berichtet, Forscher-Primärquelle). (100 %) [<https://jakkaru.de/articles/sungrow-vulnerability-exposes-gigawatts-worldwide>]
- Sungrow hält dagegen, dass kritische Aktionen wie Firmware-Updates und Gerätesteuerung eine zusätzliche Passwortabfrage verlangen, laut pv magazine auch 2FA, und dass deshalb keine Massenoperationen möglich waren. Starkloff widerspricht: Das Passwort hätte sich zurücksetzen lassen (Herstellerangabe, inhaltlich strittig). (100 %) [<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]
- Laut hessenschau waren die registrierten Anlagen samt Adressen einsehbar (berichtet). (100 %) [<https://www.hessenschau.de/wirtschaft/solaranlagen-wie-kritisch-war-die-sungrow-sicherheitsluecke-v4,sicherheitsluecke-solarbranche-100.html>]

- Sungrow hat die Logs ausgewertet und keine Ausnutzung durch Dritte gefunden, auch keine Datenabflüsse, Ausfälle oder Manipulationen. Das BSI sieht ebenfalls keine Hinweise auf Missbrauch, und ein Stromausfall ist nicht bekannt (Herstellerangabe bzw. berichtet). (100 %)

[<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Starkloff hat nach eigenen Angaben nicht an realen Anlagen getestet (berichtet). (100 %)

[<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud>]

- Laut einer DNV-Studie für SolarPower Europe (April 2025) kann schon die Kompromittierung von 3 GW Wechselrichterleistung erhebliche Folgen für das europäische Netz haben (Studie).

(100 %) [<https://taiyangnews.info/markets/solarpower-europe-dnv-cybersecurity-report>]

NICHT BEKANNT

- Ob die Passwort- bzw. 2FA-Abfrage auch für Admin-Konten galt oder sich umgehen ließ, denn Forscher und Hersteller widersprechen sich und es wurde nicht praktisch getestet.

- Wie viel Leistung tatsächlich gleichzeitig steuerbar gewesen wäre, denn nicht alle Geräte sind in der Cloud registriert und Sungrow nennt keine Zahl.

- Welche Kundendaten genau einsehbar waren und ob eine Datenschutz-Meldung erfolgt ist.

WAHRSCHEINLICH (Einschätzung)

- Die Forscher konnten Kundendaten wie Konten, Anlagen und Organisationen einsehen. Abgeflossen sind sie nach heutigem Stand nicht. (70 %) – Jakkaru spricht von Zugriff auf alle Organisationen und Nutzer, hessenschau von einsehbaren Adressen, und Sungrow stellt keinen Datenabfluss fest.

- Ein koordiniertes, unerwartetes Abschalten von deutlich mehr als 3 GW hätte das Netz ernsthaft belastet. (50 %) – Dafür sprechen die 3-GW-Auslegung und die Einschätzung von Fraunhofer (Wickert: „akute Blackout-Gefahr“ bei 17 GW). Offen ist aber, ob der Steuerweg funktioniert hätte, und Tennet und Amprion verweisen auf ihre Reserven (widersprüchlich: A 60 % / B 50 %).

- Ein europaweiter Blackout wäre die sichere Folge gewesen. (15 %) – Dafür hätten sowohl die Umgehung der Zusatzabfrage als auch der synchrone Massenbefehl gelingen müssen, und beides ist unbewiesen. Die Wirkung hängt außerdem von Tageszeit und Netzlage ab, und der ENTSO-E-Bericht zu Iberien 2025 zeigt, dass solche Ausfälle aus mehreren Faktoren entstehen.

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

WISSEN

- Gemeldet wurde die Lücke am 22.08.2026. Am 25.08.2026 spielte Sungrow einen Notfall-Patch auf allen Ebenen der Plattform ein, und Mitte September konnte Jakkaru sie bei einem Nachtest nicht mehr nachstellen (Herstellerangabe, berichtet). (100 %)

[<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Laut Starkloff war die Lücke einen Tag nach der Meldung geschlossen (berichtet). (widersprüchlich: Starkloff 1 Tag / Sungrow Notfall-Patch nach 3 Tagen; Sungrow sagt auch, die Ursache sei am selben Tag behoben gewesen) (100 %) [<https://www.tagesspiegel.de/wirtschaft/dpa-hacker-hatte-hunderttausende-solaranlagen-in-deutschland-lahmlegen-konnen-16137653.html>]

- Laut pv magazine müssen Kunden und Installateure nichts weiter tun (berichtet). (100 %)

[<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Sungrow hat die NCC Group mit einer Sicherheitsprüfung beauftragt (Herstellerangabe). (100 %) [<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Zum Vergleich: CVE-2025-29756 wurde auf dem Server behoben, ohne dass Kunden etwas tun mussten (bestätigt, Sungrow-Advisory). (100 %)

[<https://www.sungrowpower.com/en/security-notice-detail-2/6593>]

- Für die Forescout-Lücken (ICSA-25-072-12) waren dagegen ein WiNet-Firmware-Update ab WINET-SV200.001.00.P028 und ein App-Update nötig (bestätigt). (100 %)

[<https://cisa.gov/news-events/ics-advisories/icsa-25-072-12>]

NICHT BEKANNT

- Ob Sungrow Behörden und Kunden aktiv informiert hat, denn diese Frage blieb laut dpa unbeantwortet.
- Ob Sungrow alle Sitzungen und Zugangsdaten aus dem verwundbaren Zeitraum zurückgesetzt hat.
- Wann die Prüfung durch die NCC Group abgeschlossen ist.

WAHRSCHEINLICH (Einschätzung)

- Weil der Fix zentral in der Cloud lief, gab es für die Betreiber digital nichts wiederherzustellen. (80 %) – Es war ein Login-Fehler auf dem Server, und Hersteller und pv magazine sagen, dass Kunden nichts tun müssen (widersprüchlich: A 80 % / B 85 %).
- Wäre über die Lücke manipulierte Firmware verteilt worden, hätte die Bereinigung Wochen bis Monate gedauert, teils mit Einsätzen vor Ort. (45 %) – Das ist hypothetisch. SolarFlareSec hat 2024 ein solches Firmware-Szenario gezeigt, aber für diese Größenordnung gibt es keinen realen Präzedenzfall.

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

WISSEN

- Laut Sungrow gab es keine Unterbrechungen und keine unautorisierten Manipulationen an Kundenanlagen (Herstellerangabe). (100 %)

[<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Die Installationsbetriebe melden keinen Datenabfluss und keine Manipulation (berichtet). (100 %) [<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud>]

- Ein Stromausfall wegen der Lücke ist nicht bekannt (berichtet). (100 %) [<https://www.tagesspiegel.de/wirtschaft/dpa-hacker-hatte-hunderttausende-solaranlagen-in-deutschland-lahmlegen-konnen-16137653.html>]

- Im Projekt SolarFlareSec zeigte ein Forscher 2024, dass manipulierte Firmware Komponenten der Wechselrichter wie Netzschutz-Relais beeinflussen kann. Belegt ist dort das Abschalten zu einem bestimmten Zeitpunkt, nicht eine dauerhafte Zerstörung (Forscher-Primärquelle, früherer Fall). (100 %) [<https://veganmosfet.codeberg.page/posts/2024-04-21-solarflaresec/>]

NICHT BEKANNT

- Ob es eine unabhängige Prüfung gibt, dass keine Firmware verändert wurde.
- Ob ein Angreifer über diesen Weg Hardware dauerhaft hätte beschädigen können, denn das wurde nicht getestet.

WAHRSCHEINLICH (Einschätzung)

- An den Anlagen ist durch diesen Fall physisch nichts beschädigt. (90 %) – Hersteller, BSI und Installationsbetriebe sehen keine Ausnutzung, es wurde kein Ausfall gemeldet, und der Forscher hat nicht an realen Anlagen getestet.
- Ein reines Abschalten über die Cloud hätte vor allem Ertragsausfall bedeutet und keine dauerhaften Hardware-Schäden. (65 %) – Starten und Stoppen sind reguläre Funktionen. Gefährlicher wären manipulierte Firmware oder Schutzeinstellungen, und das bleibt hypothetisch.
- Böswillige Firmware hätte Wechselrichter so unbrauchbar machen können, dass sie vor Ort getauscht oder neu bespielt werden müssen. (35 %) – Technisch ist das denkbar, belegt ist bisher aber nur das zeitgesteuerte Abschalten.

5. Wie viele solcher Ziele gibt es?

WISSEN

- In Deutschland laufen rund 250.000 PV-Anlagen mit Sungrow-Wechselrichtern, die an der Cloud hängen (berichtet). (100 %) [<https://www.computerbase.de/news/smart-home/250-000-anlagen-in-deutschland-luecke-in-cloud-von-solar-anbieter-haette-zu-blackout-fuehren-koennen.99717/>]

- Laut Jakkaru hat Sungrow weltweit über 1.000 GW Leistungselektronik installiert, Stand Dezember 2025 (berichtet). (100 %)

[<https://jakkaru.de/articles/sungrow-vulnerability-exposes-gigawatts-worldwide>]

- Laut SolarPower Europe/DNV kontrollieren mehr als ein Dutzend westliche und nicht-westliche Hersteller jeweils deutlich mehr als 3 GW installierte Wechselrichterleistung (Studie). (100 %)

[<https://taiyangnews.info/markets/solarpower-europe-dnv-cybersecurity-report>]

- Forescout fand 2025 im Projekt SUN:DOWN 46 Schwachstellen bei Sungrow, Growatt und SMA, und etwa 35.000 Solar-Managementoberflächen waren direkt aus dem Internet erreichbar (berichtet). (100 %)

[<https://www.forescout.com/blog/grid-security-new-vulnerabilities-in-solar-power-systems-exposed/>]

- Weitere Quelle zu SUN:DOWN (46 Schwachstellen) (berichtet). (100 %)

[<https://thehackernews.com/2025/03/researchers-uncover-46-critical-flaws.html?m=1>]

- Das BSI sieht eine Konzentration von Erzeugungsleistung auf einzelnen Plattformen, die wegen der direkten Steuerbarkeit über die Cloud systemkritisch ist (berichtet). (100 %)

[<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud>]

- Bei Sungrow ist es mindestens die dritte Cloud-Lücke: 2023/24 (veganmosfet, über das BSI gemeldet), CVE-2025-29756 (DIVD) und 2026 (Jakkaru) (bestätigt bzw. berichtet). (100 %)

[<https://csirt.divd.nl/2026/08/19/Sungrow-web-portal/>]

- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 138446 gesamt (DNP3 33442, OMRON FINS 23821, ProConOS 16426, EtherNet/IP 15797) (100 %)

NICHT BEKANNT

- Wie viele Wechselrichter in Deutschland insgesamt dauerhaft an einer Hersteller-Cloud hängen und wie viel PV-Leistung darüber steuerbar ist.

WAHRSCHEINLICH (Einschätzung)

- Auch andere große Hersteller-Clouds bilden zentrale Hebel mit mehreren GW Reichweite. (75 %) – Laut DNV-Studie liegen mehr als zwölf Hersteller über 3 GW, und Fernzugriff über die Cloud ist in der Branche üblich.

6. Kann das wieder passieren?

WISSEN

- Bei Sungrow ist es mindestens die dritte Cloud-Lücke in rund drei Jahren: 2023/24, CVE-2025-29756 und 2026 (bestätigt bzw. berichtet). (100 %)

[<https://csirt.divd.nl/2026/08/19/Sungrow-web-portal/>]

- Jakkaru empfiehlt, Nutzer- und Admin-Plattformen zu trennen (berichtet, Forscher-Primärquelle). (100 %) [<https://jakkaru.de/de/artikel/sungrow-vulnerability-exposes-gigawatts-worldwide>]

- Sungrow hat die NCC Group mit einer Sicherheitsprüfung beauftragt (Herstellerangabe). (100 %) [<https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>]

- Das BSI hält die Konzentration steuerbarer Erzeugungsleistung auf einzelnen Cloud-Plattformen für systemkritisch (berichtet). (100 %)

[<https://www.zfk.de/digitalisierung/it/sungrow-sicherheitsluecke-solar-cloud>]

NICHT BEKANNT

- Welche Konsequenzen Sungrow aus der NCC-Group-Prüfung zieht.
- Ob Regulierer zusätzliche Vorgaben für die Fernsteuerung von Wechselrichtern über Hersteller-Clouds machen.

WAHRSCHEINLICH (Einschätzung)

- Bei Hersteller-Clouds für Wechselrichter werden weitere Schwachstellen gefunden werden, bei Sungrow oder bei anderen Herstellern. (75 %) – Drei Sungrow-Fälle in Folge, 46 SUN:DOWN-Schwachstellen bei mehreren Herstellern und die von DNV beschriebene Konzentration sprechen dafür.

- Der Hebel bleibt groß, solange Steuerfunktionen und Nutzerzugang auf derselben Plattform liegen und Zugriffe nicht zusätzlich abgesichert sind. (70 %) – Das leitet sich aus der Jakkaru-Empfehlung und der beschriebenen Eskalation über Konto-Ebenen ab.

Lage

Der Kasseler Sicherheitsforscher Marlon Starkloff (Jakkaru GmbH) kam im August 2026 über einen Fehler in der Anmeldelogik der Sungrow-Cloud iSolarCloud ohne Passwort zuerst in Nutzer- und Installateurkonten und dann in Admin-Konten des Herstellers. Laut ZEIT/dpa waren etwa 470.000 Anlagen in Europa erreichbar, davon rund 250.000 in Deutschland mit knapp 8 GW Spitzenleistung (widersprüchlich: A 470.000 / B 470.000-500.000 in Europa). Sungrow bestätigt die Meldung vom 22.08.2026 und einen Notfall-Patch am 25.08.2026, eine Ausnutzung durch Dritte oder ein Stromausfall ist nicht bekannt, und ob sich Anlagen massenhaft hätten abschalten lassen, bleibt zwischen Forscher und Hersteller umstritten.

Angriff

Kein Angriff mit Schaden, sondern eine nachgewiesene und gemeldete Schwachstelle (Responsible Disclosure). Ein Logikfehler in der Anmeldung der Hersteller-Cloud iSolarCloud erlaubte den Zugriff auf Konten ohne Passwortprüfung. Darüber führte der Weg über Installateur- und Verwaltungskonten bis zu Admin-Konten des Herstellers, auf allen vier regionalen Plattformen. Der Angriffsvektor ist damit bekannt und muss nicht als Hypothese geführt werden. Gemeldet wurde am 22.08.2026, gepatcht am 25.08.2026, und eine Ausnutzung durch Dritte ist nicht bekannt. Ob sich darüber Steuerbefehle und Firmware massenhaft hätten auslösen lassen, ist strittig (widersprüchlich: Jakkaru ja / Sungrow nein wegen zusätzlicher Passwort- bzw. 2FA-Abfrage). Quellen: <https://jakkaru.de/articles/sungrow-vulnerability-exposes-gigawatts-worldwide>, <https://www.pv-magazine.de/2026/10/08/nach-hackerangriff-sungrow-schliesst-schwachstelle-in-seiner-isolarcloud/>

Täter

unbekannt – unbekannt

Früherer Stand: Erstmeldung (07.10.2026 12:12)

Wissen 40 % · wahrscheinlich 21 % · nicht bekannt 39 %

Laut einer ZEIT-Recherche, die am 07.10.2026 mehrere Medien aufgegriffen haben, kam das Kasseler Sicherheitsunternehmen Jakkaru um Geschäftsführer Marlon Starkloff im August 2026 ohne reguläres Passwort-Login bis in den Admin-Bereich der Sungrow-Cloud iSolarCloud. Von dort hätten sich demnach rund 250.000 Anlagen in Deutschland und knapp 500.000 in Europa zentral steuern lassen. Sungrow soll die Lücke innerhalb eines Tages per Hotfix geschlossen haben. In der Presse werden dabei zwei frühere, inzwischen geschlossene Sungrow-Fälle vermischt: veganmosfet/BSI 2023-24 und DIVD/Harm van den Brink mit CVE-2025-29756. Ein Ausnutzen durch Angreifer oder ein Netzausfall ist nicht bekannt. Meine Einordnung: „Was bisher ein theoretisches Szenario aus Studien und Warnungen war – etwa von Forescout und vom BSI –, ist mit Sungrow praktisch nachgewiesen: Über eine einzige Hersteller-Cloud waren hunderttausende Wechselrichter erreichbar.“ – Max Gilg, OT-Cybersecurity-Experte aus Rosenheim

Früherer Stand: Nach 24 Stunden (08.10.2026 12:40)

Wissen 54 % · wahrscheinlich 20 % · nicht bekannt 26 %

Marlon Starkloff, Geschäftsführer der Kasseler Jakkaru GmbH, kam im August 2026 über einen Fehler in der Anmeldelogik ohne Passwort bis in die Administratorkonten der Sungrow-Cloud iSolarCloud. Betroffen waren laut ZEIT-Recherche rund 470.000 Anlagen in Europa, davon 250.000 in Deutschland. Laut dem Forscher schloss Sungrow die Lücke innerhalb eines Tages nach der Meldung per Hotfix, das BSI spricht von „kurzfristig“. Ob sich die Anlagen tatsächlich hätten abschalten lassen, ist strittig: Der Forscher hält es für möglich, hat es aber nicht getestet, und Sungrow verweist auf ein zusätzliches Passwort. Eine Ausnutzung durch Angreifer oder einen Stromausfall gab es nach allem, was bekannt ist, nicht, das BSI stuft solche Plattformen aber als systemkritisch ein.

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