Public History of

Solar Energy Cyberattacks and Vulnerabilities

Security White Paper
DERSEC-SOLAR-VULNS-2.0

Jay Johnson

DER SECURITY

New in this Update

Since our first report in November 2024, we have cataloged an additional 50 CVE vulnerabilities in solar-based Distributed Energy Resource (DER) systems. According to the disclosures, these vulnerabilities exposed approximately ~45% of the world-wide solar generation (>1 TW) to cyber exploitation.

Highlighting the risks of electrical generation manipulation, a recent report from SolarPower Europe indicated that the loss of 3 GW of PV would cause significant implications on the European grid while the loss of 10 GW was estimated as the trigger point for a cascading outage [1]. In the wake of the Iberian Peninsula outage, it is important to note that several companies manage PV fleets that reach these critical penetration levels.

Further, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) "assess that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States" and Chinese threat actor "Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations" [2].

Key Takeaways

- Solar energy cybersecurity vulnerability disclosures have increased over recent years, with security gaps identified in fielded devices and cloud-based management systems. Vulnerable APIs have exposed more than 1 TW of distributed energy systems to remote control.
- Proof-of-concept malicious firmware exploits have demonstrated physical impacts to inverter hardware and upstream protection equipment. Chaining vulnerabilities could lead to extended power systems impacts.
- While cyberattacks on solar systems have not garnered significant attention, given the severity and prevalence of vulnerabilities in the solar ecosystem, there is a substantial risk of sustained, grid-impacting attacks. There is a desperate need for stronger security measures that protect solar generators, energy management systems, and electricity grids.

Background

Cybersecurity is crucial for solar energy systems to ensure the reliable and safe operation of the modern power grid. As solar energy systems become more numerous and more reliant on digital technology, they become more critical and vulnerable to cyberattacks. The risks have been discussed at length in several U.S. government reports and warnings [3][4][5].

Scope

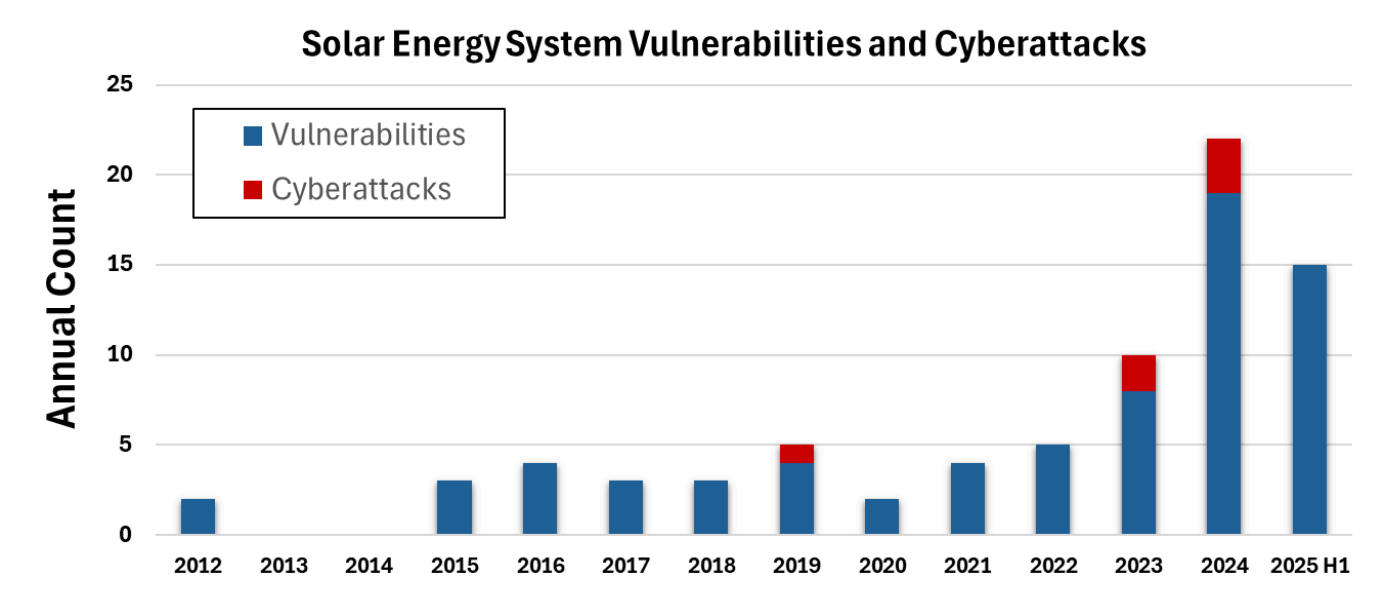
This investigation is limited to OT-specific cyberattacks and vulnerabilities that could impact PV system power monitoring or control operations, but includes an attack surface that extends to cloud-hosted management systems and the public internet [6][7]. To be included in this review, a vulnerability must enable PV system control, measurement data manipulation, firmware updates, inverter code execution, or deny access to solar telemetry. This review deliberately excluded IT or ransomware attacks on solar companies [8] or vulnerabilities associated with general-purpose PLC and SCADA equipment used with or alongside PV systems [9]. Battery systems were also excluded.

Prior Work

While a similar survey was conducted for EV chargers [10], there have been limited scientific efforts to catalogue threats to solar networks and equipment [11]. Prior DER vulnerability studies were not comprehensive or anonymized the findings [12][13]. More recently, the Forescout SUN:DOWN report provided a detailed analysis of solar vulnerabilities, impact scenarios, and attack scenarios [14]. Herein, credible solar vulnerability reports and attacks were compiled to raise awareness of this time-critical issue and encourage industry participants to engage in responsible disclosure practices.

Analysis

Our research identified 88 solar energy vulnerability disclosure "events" (disclosures grouped by affected products and security researchers) and six publicly-reported cybersecurity attacks on solar systems, shown in Figure 1 and enumerated in Table 1. The disclosures and attacks represent security findings and threat activities that have occurred across the globe.



Solar PV Attack History

2019 The first publicly disclosed solar energy cybersecurity incident was a denial-of-service attack on an unpatched Cisco firewall that prevented visibility to 500 MW of solar and wind assets operated by sPower. This event lasted for approximately 12 hours before being patched.

2023 Palo Alto Networks reported solar gateways were compromised and incorporated into Mirai botnets. In a separate incident, it was reported that Romanian solar customers modified mandatory inverter settings using installer codes to disable the voltage-active power function. This function is used by the grid operators to reduce active power at high grid voltage to keep the power system operating efficiently and safely. By modifying this grid-support function, customers made more money by not curtailing their solar systems during high voltage events but, purportedly, increased the cost of operating the power system and potentially jeopardized grid integrity as a result.

2024 Adversaries exploited remote code execution vulnerabilities in Contec SolarView Compact remote monitoring devices to incorporate them into IoT botnets. In this instance, it was reported that 800 Japanese SolarView Compact devices were hijacked and used to obscure bank account thefts that were suspected to be perpetrated by Chinese or Russian actors. This same access would have allowed the hackers to easily disable the equipment or falsify measurements from the solar installations.

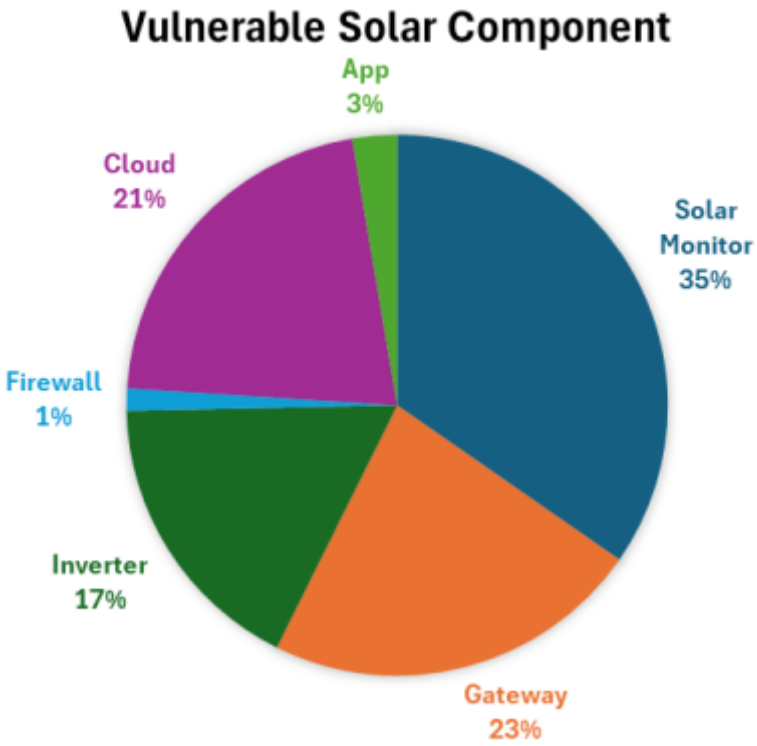
In a second incident, the Pro-Russian hacktivist group, Just Evil, targeted the Lithuanian solar monitoring solution of the state-owned energy holding company, Ignitis Group. The hacktivist group gained access to the PV monitoring platform iSolarCloud responsible for monitoring 22 small business client sites in Kaunas, Lithuania, including schools and a medical emergency station. Access was obtained using employee account information that was exposed in a data leak and the PV monitoring platform did not implement multi-factor authentication. Information about this hack was later posted on the dark web, indicating that Just Evil had temporary access to cloud-based management, monitoring, and optimization functions for the PV systems. The cloud vendor confirmed that, while credentials had been compromised, no impact was detected to the field devices.

In the third incident, according to a joint advisory from the Federal Bureau of Investigation, the Cyber National Mission Forces, and the National Security Agency, People's Republic of China-linked cyber actors compromised solar monitors for a botnet that was positioned for malicious activity.

2025 There have been no confirmed attacks on solar energy OT systems in 2025. However, additional attacks are possible given the increasing rate of vulnerability disclosures.

A Decade of Growing Cybersecurity Risk

Solar vulnerability disclosures have increased at an alarming rate recently. We found 129 unique Common Vulnerabilities and Exposures (CVEs) and other issues identified in solar energy cloud software. As shown in Figure 2, most issues were related to solar monitoring systems and gateways, with cloud infrastructure and inverters also having a sizable share of the vulnerabilities. From a risk perspective, cloud vulnerabilities would likely lead to more significant impacts because they allow attackers to control gigawatts of generation.



The total magnitude of controllable power available through this ecosystem has also grown dramatically. In 2024, the US solar industry installed nearly 50 GW of capacity to reach 239 GW [15], while the global solar capacity reached 2 TW in Nov 2024, according to the Global Solar Council [16]. This has resulted in power systems with significant instantaneous penetrations. For instance, on April 11, 2025, solar provided 26.7 GW (50.4%) of the Electric Reliability Council of Texas (ERCOT) system's total power generation [17]. In the EU, solar PV capacity reached 338 GW [18], 9% of total electricity generation [19], and had an instantaneous wind and solar penetration level of 64% [20].

Vangelis Stykas's recent cloud platform compromise demonstrations purportedly allowed him to gain access to a staggering 740 GW of generation, and perform firmware updates on many of these generation devices [21]. In the SUN:DOWN report from Forescout [22], exploit chains were presented to control or disconnect over 1 TW of solar capacity. Meanwhile, Sébastien (a.k.a. veganmosfet) has demonstrated the ability to gain unauthorized access to four different inverter types, modify the firmware of these devices, and arbitrarily control transistor switching operations [23]. Coupling the findings from these researchers, it is not difficult to imagine attacks in which 100s of GWs of solar generation are simultaneously disconnected, subsynchronous power oscillations are injected, power quality is intentionally degraded with high harmonic distortion, or all power stage switches are closed to short the DER phases and trip protection equipment. Worse, given increasing deployment of residential and light commercial battery and hybrid generation systems, additional attack scenarios are plausible outside of typical solar energy generation windows by leveraging bidirectional power flows to exceed distribution or transmission line ratings or overload transformer capacities.

Because modern solar inverters are a combination of computing devices and power conversion equipment, large-scale impacts on the grid are possible if (a) vendor, operator, or aggregator cloud systems are compromised or (b) valid firmware updates are issued that disable equipment [24][25][26]. Negative impacts can be realized with traditional cloud breaches or when attackers gain a foothold on fielded equipment and

pivot upstream. Fred Bret-Mounet demonstrated this attack vector by accessing hundreds of customer devices by compromising and escalating privileges on a Tigo Energy gateway that was connected to a virtual private network.

Given growing PV penetration and a corresponding increase in vulnerabilities, the solar industry needs to adopt stronger security protections for solar systems to prevent substantial attacks on the world's power systems. We encourage manufacturers and operators of battery energy storage systems, electric vehicle charging systems and building energy management systems to reinforce their networks for the same reason.

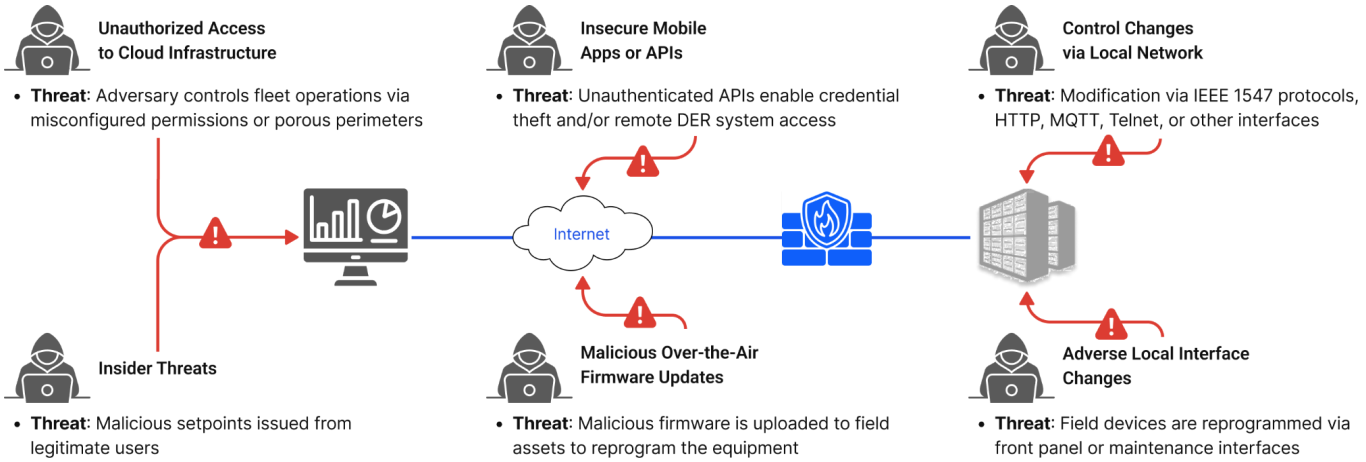


Figure 3: Solar cybersecurity threats.

Current Guidance and Regulations

Several lists of recommendations for solar cybersecurity have been curated by other organizations [27][28][29]. Unfortunately, cyber regulation in the U.S. only applies to the absolute largest solar installations with NERC CIP compliance mandates [30][31][32]. Instead of actively addressing small system vulnerabilities, including those highlighted in this paper, the country has pushed voluntary standards/guides [33], labelling programs [34], and equipment certifications [35][36] to fill a massive gap. As a result, we now have a frightening prevalence of internet-connected solar systems with default passwords and other weak security practices—often directly controlled by foreign entities that escape scrutiny or formal regulation.

EU organizations have recommended cyber-preparedness baselines for generation systems of all sizes [37] and EU regulators have implemented solar mandates via the Network and Information Security (NIS2) Directive, Cyber Resilience Act (CRA), and Network Code on Cybersecurity (NCCS) [38][39][40]. NIS2 classifies many solar operators as "essential entities" that require robust risk management, incident reporting, and vulnerability management. CRA will obligate manufacturers to conduct full lifecycle risk assessments, provide security updates, and disclose cybersecurity features and vulnerabilities of the equipment. NCCS is a set of rules that establishes a European standard for the cybersecurity of cross-border electricity flows and includes a framework of certifications, risk assessments, incident response strategies, and additional operational responsibilities for solar operators. Regulations like those in the EU are needed worldwide, especially for vendors, DER management and monitoring organizations, O&M entities, aggregators, VPPs, and other organizations with portals connected to thousands of solar generation systems.

DER Security Corp Solutions

DER Security Corp (DERSec) provides a cyber-physical anomaly detection system that uniquely protects against cyberattacks at the device, local network, and cloud levels by correlating the electrical behavior of protected assets with network control signals and out-of-band data streams. As a result, insider threats, network-based outside threats, and malicious firmware updates can be rapidly detected and mitigated. Please visit dersec.io to learn more.

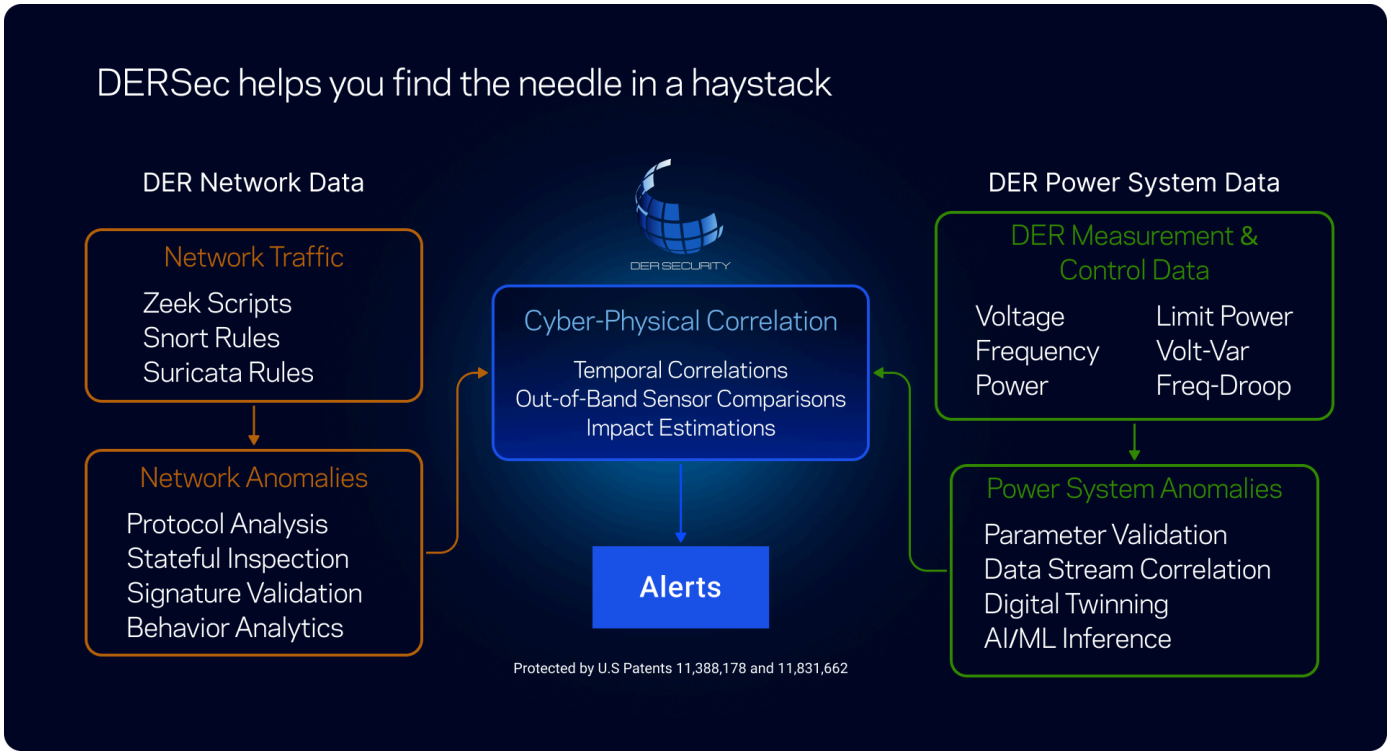


Figure 4: DERSec Cyber-Physical Intrusion Detection Solution.

Acknowledgements

We thank the security researchers for sharing their findings and the vendors for mitigating vulnerabilities described in this paper. Most vulnerabilities discussed below have been resolved but others, for which the company has gone out of business, may be unpatchable, internet-connected assets for the remainder of their lifetimes. As new vulnerabilities are discovered, responsible disclosure is essential to eliminate security weaknesses [41]. We encourage all organizations in the distributed energy ecosystem to participate in responsible disclosure practices as they help ensure the health of the industry.

Disclaimer

Information provided in this report has been obtained from public sources. The views expressed in this document are those of DERSec, which reserves the right to revise or correct any data within this document in the future. All companies listed in this document were contacted prior to publication. Many of the companies included in the document expressed support for cybersecurity transparency, responsible disclosure practices, and highlighted internal efforts to mature their solar energy cybersecurity programs.

Call To Action

Please share corrections, edits, and additions with Jay Johnson (security@dersec.io).

Table 1:

Public solar cybersecurity attacks (blue) and vulnerabilities (gray).

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
1	8/27/12	Sinapsi eSolar, eSolar DUO, eSolar Light. Sold as Schneider Electric Ezylog Photovoltaic Management Server. (Solar Monitor)	Roberto Paleari and Ivan Speziale	Unauthorized authentication via hard-coded credentials and broken session enforcement; Remote Code Execution (RCE) and Structured Query Language (SQL) injection leading to information leakage. Common Vulnerability Scoring System (CVSS) v2: 9.4, 10.0, 10.0, 7.8.	Sinapsi devices are used for monitoring/control of energy systems. Some Sinapsi devices perform building automation.	CVE-2012-5864 CVE-2012-5863 CVE-2012-5862 CVE-2012-5861	R1 R2
2	8/28/12	Carlo Gavazzi Eos-Box (Solar Monitor)	Unknown	Hard-coded passwords in the PHP file; SQL Injection. CVSS v2 10.0, 7.8	Unknown	CVE-2012-6428 CVE-2012-6427	R1
3	6/13/15	Sinapsi eSolar Light (Solar Monitor)	Maxim Rupp	Cleartext passwords visible in HTML source code of the mail-configuration page. CVSS v2: 2.1.	Unknown	CVE-2015-3949	R1
4	9/11/15	SMA Solar Sunny WebBox (Gateway)	Alexander Timorin - PT Security	Gateway has hardcoded passwords. CVSS v2: 10.0.	80,000 WebBoxes on the internet in December 2014 (but only 9,500 in Sept 2015).	CVE-2015-3964	R1 R2 R3
5	9/28/15	IBC Solar ServeMaster TLP+ and Danfoss TLX Pro+ (Inverter)	Maxim Rupp	Disclosure of application source code; plain text passwords; and cross site scripting. CVSS v2: 5.0, 5.0, 4.3.	Unknown	CVE-2015-6474 CVE-2015-6469 CVE-2015-6475	R1
6	5/14/16	Meteocontrol WEB'log. Rebranded by KACO, PowerOne, and Mastervolt. (Solar Monitor)	Karn Ganeshen	Missing authentication for application functionality and configuration pages; hidden command shell that allows running a restricted set of system commands; no CSRF Token generated per page or function. CVSS v3: 9.4, 9.4, 9.4, 9.8.	WEB'log, is a web-based SCADA system to manage energy and power equipment, including inverters.	CVE-2016-2296 CVE-2016-2297 CVE-2016-4504 CVE-2016-2298	R1 R2
7	8/1/16	Tigo Energy Maximizer Management Unit (MMU) (Gateway)	Fred Bret-Mounet	Open Wi-Fi access point; guessable username/password; poorly segmented VPN network.	Visibility/control of ~1000 Tigo MMUs on a compromised VPN connection.		R1 R2 R3
8	12/1/16	SMA Sunny Portal (Cloud); SMA SunnyBoy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 (Inverter)	Willem Westerhof	Information disclosure; hard-coded credentials; unsecured firmware updates; unauthenticated user permissions; Cross Site Scripting (XSS); poor encryption; weak password hashing; default passwords; insecure communication protocols; etc. CVSS v3: 7.5, 9.8, 9.8, 9.8, 9.8, 9.8/3.4, 8.1, 7.5, 9.8, 9.8, 9.8, 7.5, 8.8, 7.5.	These attacks require OT LAN access but affected a large portion of the 2017 SMA installed base of more than 35 GW.	CVE-2017-9851 CVE-2017-9852 CVE-2017-9853 CVE-2017-9854 CVE-2017-9855 CVE-2017-9856 CVE-2017-9857 CVE-2017-9858 CVE-2017-9859 CVE-2017-9860 CVE-2017-9861 CVE-2017-9862 CVE-2017-9863 CVE-2017-9864	R1 R2 R3 R4 R5
9	12/6/25	Locus Energy LGate (Solar Monitor)	Daniel Reich	LGate web server is vulnerable to OS command injection via a POST request to a PHP script. CVSS v3: 8.6.	US-based Locus Energy LGate devices are deployed mostly in North America.	CVE-2016-5782	R1
10	1/23/17	Solare Datensysteme GmbH SolarLog (Solar Monitor)	T. Weber - SEC Consult Vulnerability Lab	Unauthenticated password downloads and networking changes; Cross-Site Request Forgery (CSRF); arbitrary file upload; information disclosure; Denial of Service (DoS) attack disables device until restart; possible remote reprogramming. CVSS v3: 9.8/7.5, 7.5/5.3, 9.8/6.3, 7.5, 9.8/6.5, 8.8/5.3, 7.5/4.3.	Unknown	CVE-2017-20025 CVE-2017-20024 CVE-2017-20023 CVE-2017-20022 CVE-2017-20021 CVE-2017-20020 CVE-2017-20019	R1
11	4/7/17	Schneider Electric Conext ComBox (Solar Monitor)	Arik Kublanov and Mark Liapustin - Nation-E Ltd	Denial of service via resource exhaustion: three rapid sequential HTTP GET requests with a wrong username and password causes the device to self-reboot. CVSS v3: 7.5.	Conext ComBox is a communication and monitoring device for Conext XW, SW, and MPPT controllers.	CVE-2017-6019	R1 R2
12	5/18/17	Satel Iberia SenNet Solar Datalogger (Solar Monitor)	Unknown	Command injection that will allow root privileges to run arbitrary commands and change system data. CVSS v3: 8.8.	Full control over the solar monitoring system.	CVE-2017-6048	R1

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
13	7/18/17	ABB VSN300 WiFi Logger Card used with UNO and TRIO inverters (Inverter)	Maxim Rupp	Unauthorized access to internal information about status and connected devices at specific URL; ineffective privilege restrictions for “Guest” account. CVSS v3: 7.5, 6.5.	ABB UNO and TRIO series inverters were installed for years in global markets.	CVE-2017-7920 CVE-2017-7916	R1
14	8/10/17	Solar Controls WATTConfig M (Solar Monitor)	Karn Ganeshen	Uncontrolled search path element allows an attacker to execute arbitrary code on a target system using a malicious DLL file. CVSS v3: 7.8.	SCADA software runs on Windows, Ubuntu, and iOS with real-time control interface.	CVE-2017-9648	R1 R2
15	6/25/18	SAJ Solar Inverter (Inverter)	Unknown	Information leak via direct URI access. CVSS v3: 7.5.	Local data leak with OT LAN access.	CVE-2018-12735	R1
16	6/28/18	Northern Electric Power (NEP) Microinverter Gateway (Solar Monitor)	Knownsec	Sensitive information exposed via direct request to nep/status/index/1 URI. CVSS v3: 7.5.	Reconnaissance mechanism for NEP solar monitors: ZoomEye shows 258 online in Nov 2024; data leakage.	CVE-2018-12927	R1
17	10/31/18	Fronius Symo, Galvo, Eco, Primo, and Symo Advanced (Inverter); Datamanager Box 2.0 (Gateway)	T. Weber - SEC Consult Vulnerability Lab	Directory traversal; authentication bypass with "today" user account that includes daily rolling password. CVSS v3: 9.8, 6.5.	Unknown	CVE-2019-19228 CVE-2019-19229	R1
18	2/9/19	Enphase Envoy (Gateway)	pudding2	Weak password allowing access to the OS; XSS via the profileName parameter on /home; directory traversal. CVSS v3: 7.2, 6.1, 9.8.	Gateway access once on OT LAN.	CVE-2019-7676 CVE-2019-7677 CVE-2019-7678	R1
19	3/5/19	Cisco Firewall at sPower, which was acquired by AES in 2020 (Firewall)	N/A	Unpatched firewall was forced to reboot repeatedly resulting in 5-minute interruptions repeated over 12-hour period.	sPower lost visibility to ~500 MW of wind and photovoltaic assets in California, Utah, and Wyoming.		R1 R2 R3
20	4/16/19	AUO Solar Data Recorder (Solar Monitor)	Luca Chiou	XSS; system setting access by unprotected URI; authentication bypass. CVSS v3: 5.4, 9.8.	Unknown	CVE-2019-11368 CVE-2019-11367	R1 R2
21	9/3/2019	SolarMAN / iGEN Wi-Fi kits used on Omnik, Hosola, Ginlong, Kstar, Seasun, SolaX, Samil, Sofar, Trannergy, GoodWe, Power-One, and more inverters (Inverter)	Jos Wetzels - Secura	Public Wi-Fi Access Point (AP), possibly with default credentials, acts as a point of entry into private networks; using hardcoded password for HF AT (SmartConfigure Smart Link) UDP Interface or IOTService Telnet port on Shanghai Hi-Flying Technology’s HF-A11 embedded Wi-Fi module allows upgrading firmware, stealing or modifying Wi-Fi configuration data, web server credentials, device info, setting GPIO pin states, and URL navigation.	The Wi-Fi kits are used on a wide range of solar products.		R1
22	10/8/19	SMA Sunny WebBox (Gateway)	Borja Merino and Eduardo Villaverde – U. of León	Cross-Site Request Forgery (CSRF) would allow attackers to impersonate the current user and generate a denial-of-service condition, modify passwords, enable services, achieve man-in-the-middle, and modify input parameters. CVSS v3: 8.8.	Unknown	CVE-2019-13529	R1 R2
23	1/23/20	Sungrow Inverters with Wi-Fi Dongles, e.g., WiNet-S or WiNet-S2 (Inverter)	Anonymous	Insecure Wi-Fi hotspot leaked home Wi-Fi password; access allows modification of inverter settings and tampering of inverter telemetry. CVSS v3.1: 5.3.	Access to a single device when in range of the Wi-Fi network.		R1 R2 R3
24	11/17/20	Tesla Backup Gateways and Powerpacks (Gateway)	Derek Abdine	API access without authentication leaking information; further API access by brute forcing default password.	379 total unique Tesla Backup Gateways have been found online.		R1 R2
25	2/17/21	Tesla/SolarCity Solar Monitoring Gateway from Digi International ConnectPort X2e (Gateway)	Jake Valletta and Sam Sabetan - FireEye Mandiant	Hardcode credentials in software; privilege escalation via symbolic link attack. CVSS v3: 8.8, 7.8.	Using the hardcoded credentials, an attacker can connect to any X2e device to extract sensitive information, install a persistence mechanism, escalate privileges, or cause denial of service conditions.	CVE-2020-9306 CVE-2020-12878	R1 R2

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
26	2/25/21	Contec SolarView Compact (Solar Monitor)	K. Okada, K. Yoshioka, T. Sasak, T. Sasaki - Yokohama National University	Get directories, files, and settings; alter settings without administrative privileges; execute arbitrary OS commands; upload arbitrary files including PHP scripts that can be executed; ability to delete arbitrary files and directories. CVSS v3: 4.3, 5.4, 9.8, 8.8, 6.1, 8.1, 7.5.	Used by 30,000 PV sites total. 615 found online.	CVE-2021-20656 CVE-2021-20657 CVE-2021-20658 CVE-2021-20659 CVE-2021-20660 CVE-2021-20661 CVE-2021-20662	R1
27	5/17/21	Enphase Envoy (Gateway)	Waylon Grange	Password derived username and serial number; default admin password for certain versions set to the last 6 digits of the serial number; hardcoded web-panel login passwords for the installer and Enphase accounts; ability to falsify production data and solar renewable-energy certificate (SREC) credits. CVSS v3: 8.8, 7.5, 9.8, 5.3.	Gateway access once on OT LAN.	CVE-2020-25755 CVE-2020-25754 CVE-2020-25753 CVE-2020-25752	R1 R2
28	6/11/21	Solar-Log GmbH Solar-Log (Solar Monitor)	Luca Chiou	Unprotected storage of credentials; missing authentication. CVSS v3: 6.5, 7.5.	Access to 10,000 devices on the internet.	CVE-2021-34544 CVE-2021-34543	
29	1/13/22	Solar-Log GmbH Solar-Log (Solar Monitor)	Cyble	No passwords or outdated firmware, vulnerable to CVE-2001-1341, enabled information disclosure, cross-site request forgery, unauthenticated arbitrary file upload, unauthenticated change of network configurations, system compromise, and denial of service risk.	Cyble found 900 internet-connected devices, with >20 vulnerable instances.		R1
30	5/15/22	Contec SolarView Compact (Solar Monitor)	Ahmed Alroky - Alactive	Directory traversal; local file disclosure via */html/Solar_Ftp.php*; command injection via *conf_mail.php* in SolarView Compact v6.00. CVSS v3: 7.5, 5.5, 9.8.	Used by 30,000 PV sites total. 615 found exposed online with 425 of those running unpatched versions.	CVE-2022-29298 CVE-2022-29302 CVE-2022-29303	R1 R2 R3 R4 R5
31	5/18/22	Contec SolarView Compact (Solar Monitor)	badboycxcc	XSS via *Solar_AiConf.php* in SolarView Compact v6.0. CVSS v3: 6.1.	Used by 30,000 PV sites total. 615 found online.	CVE-2022-31373	R1
32	7/24/22	IGEN Tech SOLARMAN Website affecting SOLARMAN/Solis/ Omnik/Ginlong converters, loggers, & batteries (Cloud)	Jelle Ursem, Célistine Oosting, Frank Breedijk - DIVD	Super Admin account password was found on a GitHub repository for all sites that exposed GPS coordinates, current and historical production data, faults, and the ability to clear faults, upload and download firmware, and create/delete users.	SOLARMAN platform has almost 1,000,000 plants (~10GWp).	DIVD-2022-00009	R1
33	7/29/22	Inavitas Solar Log (Solar Monitor)	Unknown	SQL Injection vulnerability. CVSS v3: 9.8/9.4.	Unknown	CVE-2022-1277	R1
34	8/2/22	Solar-Log GmbH Solar-Log (Solar Monitor)	Andrea D'Ubaldo, Antonio Montillo - Swascan	Backdoor accounts for administrators to adjust configuration settings, communications, etc. CVSS v3: 9.8.	Data falsification or bricking of 10,000 devices on the internet.	CVE-2022-47767	R1
35	10/17/22	Kostal PIKO MP (Inverter)	David de Paula Santos	XSS via file upload feature.	Unknown	CVE-2022-42974	R1
36	10/26/22	Contec SolarView Compact (Solar Monitor)	Eslam Kamal (strik3r0x1)	Unrestricted file uploads for SolarView Compact 4.0 & 5.0; XSS in SolarView Compact before v7.00. CVSS v3: 9.8, 6.1.	Used by 30,000 PV sites total. 615 found online.	CVE-2022-44354 CVE-2022-44355	R1
37	2/5/23	Contec SolarView Compact (Solar Monitor)	Timorlover	Command injection via *network_test.php* in SolarView Compact 6.00; command injection via *downloader.php* in SolarView Compact v6.00 and before. CVSS v3: 9.8, 9.8.	Used by 30,000 PV sites total. 615 found online.	CVE-2022-40881 CVE-2023-23333	R1 R2
38	2/9/23	Altenergy Power System, Inc. (APsystems) Energy Communication Unit ECU-R (Gateway)	Stan de Boer (0xst4n)	Command injection in the timezone parameter of the administration interface allows root RCE. CVSS v3: 9.8.	Palo Alto Networks' Unit 42 reports this vulnerability was leveraged by the Mirai botnet.	CVE-2022-45699	R1 R2 R3
39	2/13/23	Deye, Revolt, or Bosswerk MW3_15U_5406_1.47/471 (Inverter)	Unknown	Hard-coded credentials for the Wi-Fi access point cannot be changed. CVSS v3: 6.8/3.9.	Unknown	CVE-2023-0808	R1

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
40	3/14/23	Altenergy Power System, Inc. (APsystems) ECU (Gateway)	Ahmed Alroky - Alactive	Altenergy Power Control Software vulnerable to timezone command injection at */index.php/management/datetime*. CVSS v3: 9.8.	Full remote access to gateway operating system.	CVE-2023-28343	R1 R2 R3
41	4/15/23	Sungrow iSolarcloud (iSC) (Cloud)	Anonymous	Unauthenticated users can create SuperAdministrator, with (a) permissions to read, delete, or modify any user account within iSC, and (b) read, delete, or modify any plant within iSC.	Full access to the entire fleet.		R1
42	5/8/23	Contec SolarView Compact (Solar Monitor)	Chuya Hayakawa - 00One, Inc.	Hard-coded credentials before v8.10; OS command injection via download page before v8.10; buffer overflow and RCE on multiple setting pages before v8.10; Command injection on mail setting prior to v8.10; access to OS date/time prior to v8.10. CVSS v3: 7.2, 8.8, 8.8, 6.5, 8.8.	Used by 30,000 PV sites.	CVE-2023-27512 CVE-2023-27514 CVE-2023-27518 CVE-2023-27920 CVE-2023-27521	R1
43	5/8/23	Contec SolarView Compact (Solar Monitor)	xiaosed	Any file on the server can be read or modified using *texteditor.php*. CVSS v3: 9.1/9.8.	Used by 30,000 PV sites.	CVE-2023-29919	R1
44	6/20/23	Enphase IQ Gateway (Gateway)	OBSWCY3F	Command injection; information leak via hard-coded credentials embedded in binary code in Enphase Installer App. CVSS v3: 9.8/6.3, 7.5/8.6.	Customer sensitive data leaks or remote gateway control.	CVE-2023-33869	R1
45	6/27/23	Enphase Installer App (App)				CVE-2023-32274	
46	9/1/23	Hoymiles Microinverter HM-300 with DTU-Lite (Inverter); Hoymiles website (Cloud)	Sebastien, AKA veganmosfet	Missing cloud API authorization allowing data extraction; ability to upload arbitrary firmware image on cloud; Insecure Direct Object Reference (IDOR) to execute commands on any inverter remotely such as triggering malicious firmware updates; no TLS for cloud inverter-to-cloud communications; missing secure boot and secure debugging.	Ability to remotely update firmware on 300,000 Hoymiles power plants, enabling the ability to turn on/off devices and change switching control to change power factor or short phases (tripping protection equipment).		R1
47	10/16/23	Growatt MIC600TL-X with ShineWIFI-X Stick (Inverter); Growatt Server (Cloud)	Sebastien, AKA veganmosfet	Manipulated firmware can be installed locally or remotely (IDOR, insecure communications, no code signing, Wi-Fi stick serial number leak); cloud API traffic from the Wi-Fi stick can be redirected to any IPv4 address.	Full control over all inverter connected to the cloud. Malicious firmware was uploaded to control the inverter transistors.		R1
48	10/30/23	Solar-Log GmbH Solar-Log (Solar Monitor)	Vincent McRae, Mesut Cetin - RedTeamer IT Security	Stored XSS in 3.6.0 web panel could allow privilege escalation. CVSS v3: 5.4.	PrivEsc for 10,000 devices on the internet.	CVE-2023-46344	R1 R2
49	11/12/23	SolaX X1 Microinverter with SolaX Pocket WiFi 3.0 (Inverter); solaxcloud (Cloud)	Sebastien, AKA veganmosfet	Admin privileges on cloud platform; extract sensitive personal data; MQTT broker data spoofing including changing inverter settings and pushing remote malicious firmware updates.	Extract data and manipulate settings (on/off, etc.) for 350,000 devices, leak personal account details, update all firmware inverter images.		R1
50	12/26/23	Unknown Products (Inverter)	PV Owners	Installer-level credentials are used to modify the Romanian volt-watt function in the inverter to produce more energy during high grid voltage.	Grid-support function is disabled, making the power system more difficult and expensive to operate according to the National Energy Regulatory Authority (ANRE).		R1
51	12/27/23	Sungrow SG RS string inverter with WiNet-S (Inverter); iSolarCloud (Cloud)	Sebastien, AKA veganmosfet	Extract sensitive data for all devices/users (e.g., API call to fetch Wi-Fi password for any serial number); ability to trigger firmware updates; manipulated firmware images could be pushed to the cloud with malicious relay operations (no code signing).	350,000 registered users in EU; >10 GW connected to the compromised European server.		R1

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
52	1/11/24	Enphase IQ Envoy (Gateway)	Charles Perine, Philippe Z Lin, Lord Remorin, and Josiah Hagen - Trend Micro and Casey Colando - All Energies	Computed default “installer” password based on the gateway serial number which enables de-energization, microinverter/battery disassociation, and nearby Wi-Fi Access Points.	4.7 million Enphase systems with 80 million microinverters have been deployed in more than 160 countries.		R1
53		Sol-Ark PowerView WiFi Plus Ethernet Dongle (Gateway)		No authentication for web endpoint which can be used to get the inverter serial number, Wi-Fi dongle key, and other data, permits remote reboots, and nearby Wi-Fi Access Points; clear-text command to trigger firmware update and unencrypted HTTP firmware download; unencrypted connection to Alibaba cloud includes serial number, Wi-Fi dongle key, Wi-Fi password, model name, firmware version, etc.	Sol-Ark has more than 40,000 customers.		
54		Victron Energy Cerbo GX (Gateway)		Default, no-password for front panel and built-in noVNC service which allows remote firmware upgrades and device shut down operations.	Victron Energy has over 1 million customers and installers in 100 countries.		
55	1/28/24	Growatt v8.1.0.0	l00neyhacker	Access sensitive information or execute injection attacks.	Potential cleartext downgrade attack.	CVE-2024-22678	R1
56	2/26/24	SMA Sunny Webbox (Gateway)	Unknown	Clickjacking vulnerability in gateway website where an attacker could lure a user to click on a malicious URL. CVSS v3: 6.4.	Product’s end-of-life was 12/31/2015.	CVE-2024-1890	R1
57	2/26/24	SMA Cluster Controller (Gateway)	Unknown	Cross Site Request Forgery (CSRF, XSRF) vulnerability in SMA Cluster Controller. CVSS v3: 5.4/6.4.	Product’s end-of-life was 6/30/2018.	CVE-2024-1889	R1
58	3/21/24	SolarEdge mySolarEdge (App)	Tobias Jäger - SySS GmbH	Missing certificate verification allows app-to-cloud Machine-in-the-middle (MitM) attacks that can read and falsify exchanges. CVSS v3: 5.9.	MITM attacks of customers using the app.	CVE-2024-28756	R1 R2
59	4/11/24	Enphase IQ Gateway (Gateway)	Wietse Boonstra, Hidde Smit, Max van der Horst, and Frank Breedijk - DIVD	OS command injection via URL, package upload, or elements used by internal scripts; directory traversal. CVSS v4: 8.6, 8.6, 8.7, 9.2, 9.2, 9.3.	RCE of gateways, some of which may be connected to the public internet.	CVE-2024-21881 CVE-2024-21880 CVE-2024-21879 CVE-2024-21878 CVE-2024-21877 CVE-2024-21876	R1 R2
60	5/1/24	Contec SolarView Compact (Solar Monitor)	South Korean security company S2W attributed the attack to Arsenal Depository, a.k.a. Hacker CN, which is likely Chinese or Russian.	800 Contec SolarView Compact SV-CPT-MC310 remote monitoring devices were hijacked to support bank account thefts.	No known impact on the power system; access to the site network; financial impacts for affected banks; possible performance impacts (e.g., extended response time, heavier processor usage) for the monitoring devices.	The cyberattack purportedly exploited CVE-2022-29303	R1 R2 R3 R4
61	5/22/24	IGEN Tech SOLARMAN Website (Cloud)	Ioan Melniciuc, Alexandru Lazar, George Cabau, and Radu Basaraba - BitDefender	Takeover of the business (contractor) account used by the authorized installation company to control devices, modify voltage or frequency controls/settings; JWT token reuse, and PII and other data leaks.	195 GW, or roughly 20% of the global solar power production. SOLARMAN partner companies include Deye, Afore, Canadian Solar, Sofar, Intelbras, Havells, Anfuote, Beyondsun, Fxpower, Itramas, Yienergy, Malina, and Trannergy which each needed to patch.		R1 R2 R3
62	5/22/24	Deye Cloud/Website (Cloud)		Hard coded credentials; information leakage.			

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
63	6/27/24	IGEN Tech SOLARMAN Website (Cloud)	Vangelis Stykas - Atropos	Admin access; firmware update capability via Insecure Direct Object Reference (IDOR), Remote Command Execution, and Broken Authorization.	Access to several 100s of GWs of PV generation, personal data, administrative accounts and panels, ability to brick inverters, and access to internal networks.		R1 R2 R3 R4
64		Sunsynk Website (Cloud)					
65		Solax Website (Cloud)					
66		Growatt Website (Cloud)					
67		Ingecon SUN Website (Cloud)					
68		Fox ESS Customer Website (Cloud)					
69	7/26/24	Solar-Log GmbH Solar-Log (Solar Monitor)	Nepenthe 0320	Solar-Log 1000 lacks authentication for some URIs; authentication bypass; password leaks for FTP, SMTP, and SMS. CVSS v3: 8.1, 9.8.	Solar-Log1000 monitors up to 100 inverters with a total output of up to 1 MWp.	CVE-2024-40116 CVE-2024-40117	R1 R2
70	8/7/24	GivEnergy Home Assistant API (Virtual Power Plant Cloud)	Ryan Castellucci	Unauthorized access to GivEnergy accounts by brute force factorization of the 512-bit RSA API key.	Access to 200 MW of programmable capacity.		R1 R2 R3
71	9/13/24	User credentials stolen for Sungrow iSolarCloud (Cloud)	N/A	Pro-Russian hacktivist group, Just Evil, targeted Lithuanian solar monitoring solutions of state-owned Energy holding company Ignitis Group.	Access to 22 compromised client sites owned by schools and medical emergency stations.		R1
72	9/18/24	Contec SolarView Compact (Solar Monitor)	N/A	People's Republic of China (PRC)-linked cyber actors have compromised Contec solar monitors to create a botnet "positioned for malicious activity" using a Mirai-based malware payload.	Integrity Technology Group compromised over 260,000 devices, although it's unknown how many were Contec solar monitors.	CVE-2022-40881 CVE-2023-23333	R1
73	9/17/24	Altenergy Power System, Inc. (APsystems) ECU (Gateway)	h0e4a0r1t	SQL injection allows arbitrary database operations on Altenergy Power Control Software via *date* parameter in *get_status_zigbee* function. CVSS v4: 5.3.	45 devices were exposed online according to nuclei scan 11/8/24.	CVE-2024-11305	R1
	11/8/24			All databases in the Altenergy Power Control Software can be viewed at */index.php/display/database/*. CVSS v4: 6.9.		CVE-2024-11306	R1
74	11/27/24	SMA Sunny Central Line (Inverter)	Unknown	Authenticated SQL injection on the administration panel allowing access to a database. CVSS v3: 5.4.	58 Sunny Central inverter product types were affected by this vulnerability.	CVE-2024-11025	R1
75	2/13/25	Outback Power Mojave (Inverter)	Jon Hurtado, Jay Johnson, Brian Wright – Sandia National Laboratories	GET request method with sensitive query strings; exposure of sensitive information to an unauthorized actor; operating system command injection via specially-crafted post requests. CVSS v4: 8.7, 8.7, 8.7.	Outback power has an install base of over 300 MW of energy- efficient solar systems and battery storage.	CVE-2025-26473 CVE-2025-25281 CVE-2025-24861	R1
76	3/5/25	SMA SunnyBoy (Inverter)	Ahmed Alroky - Alactive	Directory traversal vulnerability in SMA Sunny Boy v3.0, Firmware 1.1.32.R.	SMA has an installed solar inverter capacity of 132 GW.	CVE-2025-29572	R1

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Impact	CVEs	Ref
77	3/27/25	SMA SunnyPortal (Cloud)	Stanislav Dashevskyi, Francesco La Spina, Daniel dos Santos - Forescout	Unauthenticated execution of uploaded *.aspx* files on *sunnyportal.com*. CVSS v3: 8.8.	SMA has an installed solar inverter capacity of 132 GW.	CVE-2025-0731	R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11
78		Growatt (Cloud)		Stored XSS vulnerability in *server.growatt.com.* CVSS v4: 8.7.	Growatt is the world's largest residential inverter supplier with over 3 million end users connected to their cloud platform and systems installed in over 180 countries. Growatt has approximately 300 GW of generating capacity. These vulnerabilities would allow an attacker to control all internet-connected Growatt assets.	CVE-2025-30511	
79		Growatt (Cloud)		Exposed API allows username enumeration; authenticated user info leaks of plants and devices that belong to other users and infer other usernames; smart meter serial number and email address leaks. CVSS v4: 6.9, 6.9, 6.9, 6.9, 6.9, 6.9, 6.9, 8.7, 6.9, 6.9, 6.9, 6.9, 6.9, 6.9, 6.9, 6.9.		CVE-2025-24487 CVE-2025-24850 CVE-2025-25276 CVE-2025-27561 CVE-2025-27565 CVE-2025-27568 CVE-2025-27938 CVE-2025-27939 CVE-2025-30254 CVE-2025-30257 CVE-2025-30514 CVE-2025-31357 CVE-2025-31360 CVE-2025-31654 CVE-2025-31933 CVE-2025-31941 CVE-2025-31949	
80		Growatt (Cloud)		Manipulate other users' smart home setups and hijack/ rename devices by allocating them to another account. CVSS v4: 6.7, 6.7.		CVE-2025-26857 CVE-2025-27719	
81		Growatt (Cloud)		Attackers can upload arbitrary files in place of the plant's image at *server.growatt.com/energy/ updatePlant* and then access them via a specific URL in Growatt cloud. CVSS v4: 9.3.		CVE-2025-30510	
82		Growatt (Cloud)		Attackers can inject malicious JavaScript code into users personal spaces and possibly other places of the *energy.growatt.com* portal. CVSS v4: 9.3.		CVE-2025-24297	
83		Sungrow (App)		The Android app for iSolarCloud explicitly ignores certificate errors and is vulnerable to MitM attacks, where an attacker may impersonate the iSolarCloud; Android mobile application uses an insecure AES key to encrypt client data. CVSS v4: 8.3, 8.3.	Sungrow's installed capacity of inverter and converter equipment worldwide exceeds 740 GW. These vulnerabilities would allow an attacker to control all internet-connected Sungrow assets.	CVE-2024-50691 CVE-2024-50684	
84							
85		Sungrow App and iSolarCloud (App/Cloud)		The Android application and the cloud use hardcoded MQTT credentials for exchanging the device telemetry. CVSS v4: 6.9.		CVE-2024-50688	
86		Sungrow iSolarCloud (Cloud)		Multiple insecure direct object references (IDOR) via the *powerStationService*, *userService*, *orgService*, *commonService*, and *devService* API models. CVSS v4: 6.9, 6.9, 6.9, 9.2, 9.2.		CVE-2024-50685 CVE-2024-50686 CVE-2024-50687 CVE-2024-50689 CVE-2024-50693	
87		Sungrow WiNet (Gateway)		Potential stack-based buffer overflows when copying timestamp from an MQTT message, when decrypting MQTT messages with specific TLV fields, and collecting MQTT topics; potential heap-based buffer overflow without MQTT message content bounds checks; WiNet's module firmware contains hardcoded MQTT credentials that allow broker impersonation; WiNet WebUI contains a hardcoded password that can be used to decrypt all firmware updates. CVSS v4: 9.5, 9.5, 9.5, 9.5, 9.5, 6.5.		CVE-2024-50694 CVE-2024-50695 CVE-2024-50697 CVE-2024-50698 CVE-2024-50692 CVE-2024-50690	
88		Sungrow Inverters (Inverter)		Possible to update inverters with arbitrary firmware via MQTT (no integrity check). CVSS v4: 8.1.		CVE-2024-50696	