Public History of Solar Energy Cyberattacks and Vulnerabilities

Jay Johnson, DER Security Corp

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 [1][2][3].

Scope: This investigation is limited to OT-specific cyberattacks and vulnerabilities that could impact PV site power monitoring or control operations, but includes an attack surface that extends across cloud-hosted management systems and the public internet [4][5]. To be catalogued, the vulnerability/attack enabled malicious control of the PV system, measurement manipulation, firmware updates, inverter code execution, or deny access to solar telemetry. This summary deliberately excluded IT or ransomware attacks on solar companies [6] or vulnerabilities associated with general-purpose PLC and other SCADA equipment used with or alongside PV systems [7].

Prior Work: While a similar study was previously conducted for EV chargers [8], there have been limited academic efforts to catalogue threats to solar networks and equipment [9]. Generally, prior DER vulnerability studies were noncomprehensive and/or anonymized their findings [10][11]. Herein, credible solar vulnerabilities and attacks have been compiled in hopes of raising awareness of this time-critical issue and encouraging industry participants to engage in responsible disclosure practices.

Analysis: Our research identified four publicly-reported cybersecurity attacks on solar systems and 50 solar energy vulnerability disclosure events—loosely grouped by affected product(s) and security researcher(s)—as shown in Figure 1 and Table 1. The disclosures and attacks represent a range of events that have occurred across the globe.

In March 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.

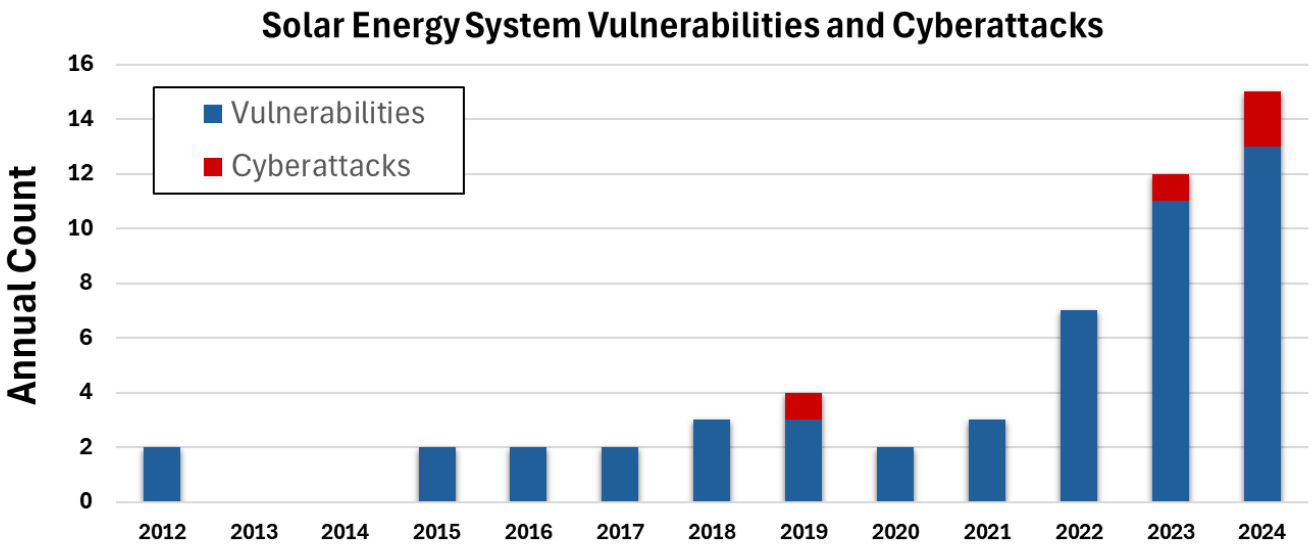

Figure 1: Solar cybersecurity reports binned by year.

In 2023, it was reported that Romanian solar customers modified mandatory inverter settings using installer codes to disable the voltage-active power function. This function is required by the Romanian 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, these 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.

In 2024, two attacks were reported. First, adversaries exploited remote code execution vulnerabilities in Contec SolarView Compact remote monitoring devices to add these devices to IoT botnets which executed nefarious commands. 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 separate incident, the Pro-Russian hacktivist group, Just Evil, targeted Lithuanian solar monitoring solutions of state-owned energy holding company, Ignitis Group. One leading theory is that the threat actor gained access to the 22 compromised client sites, including hospitals and military academies, by acquiring valid credentials to the owner's PV Monitoring Platform using a Trojan on the customer's computers or phones. This information was later posted on the dark web. Just Evil had temporary access to cloud-based management, monitoring, and optimization functions for the PV systems. The cloud vendor confirmed with the customer that while credentials had been compromised, no attacks were detected on the fielded devices.

Since coming into view in 2012, solar vulnerability disclosures have increased at an alarming rate. These include 79 Common Vulnerabilities and Exposures (CVEs) as well as other issues identified in solar energy cloud software. As shown in Figure 1, the rate of cyberattacks and vulnerability disclosures has increased during the past three years. Compiling all reports, the majority were related to solar monitoring systems or cloud infrastructure—as shown in Figure 2—with inverters and gateways also having a sizable share of the vulnerabilities.

At the same time, the total magnitude of controllable power available through these systems has grown dramatically. Vangelis Stykas's recent cloud platform compromises purportedly allowed him to gain access to a staggering 740 GW of generation, along with the ability to perform firmware updates on many of these generation devices. Meanwhile, Sébastien (a.k.a. veganmosfet) has demonstrated the ability to gain unauthorized access to four different inverters to modify the firmware of these devices and arbitrarily control transistor switching operations. 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 THD, or all H-bridge switches are closed to short 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, such as leveraging bidirectional power flows to exceed distribution or transmission line ratings or overload transformer capacities.

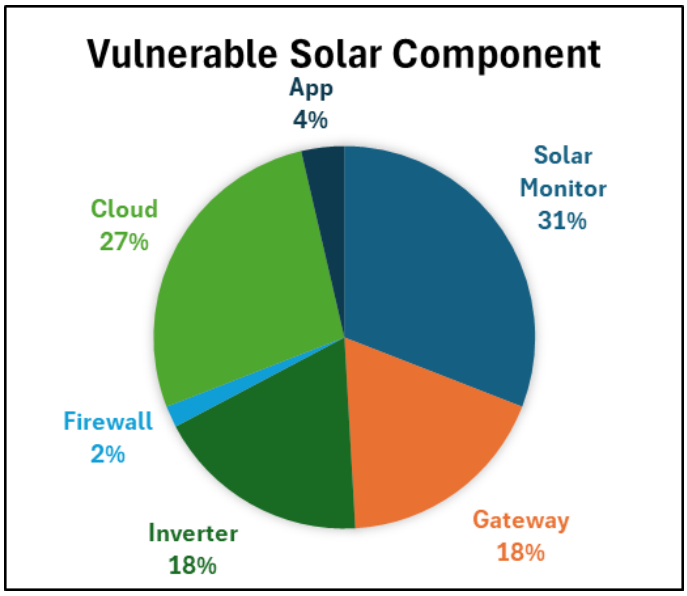

Figure 2: Solar component identified in the vulnerability disclosure or targeted in the cyberattack.

In many ways, modern solar inverters are simply IoT devices connected to power conversion equipment.

This means physical grid impacts are possibly on a grand scale if vendor, operator, or aggregator cloud systems are compromised. This risk can be realized with traditional cloud breaches but also if attackers gain a foothold on fielded equipment and pivot upstream. Fred Bret-Mounet demonstrated this attack vector by gaining VPN network access by gaining root access to a Tigo Energy gateway. Given these risks, the solar industry needs stronger security for solar systems and must better protect upstream and downstream data exchanges to prevent substantial attacks on the world's power systems. We expect other types of grid-edge equipment (electric vehicle chargers, building systems, etc.) to follow suit as the ubiquity of those technologies also reaches grid-critical risk levels.

Current Guidance and Regulations: Several lists of recommendations for solar cybersecurity have been curated by many different organizations [12][13][14]. Unfortunately, cyber regulation in the U.S. only applies to the absolute largest solar installations [15][16][17]. Instead of actively addressing small system vulnerabilities, including those highlighted in this paper, the country has pushed voluntary standards/guides [18], labelling programs [19], and equipment certifications [20][21] 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 [22] 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) [23][24][25]. NIS2 classifies many solar operators as "essential entities" which requires 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.

DERSec Solutions: DERSec offers cyber-physical anomaly detection systems that uniquely protect against cyberattacks at the device, local network, and cloud levels by correlating diverse out-of-band data streams with system behaviors and network traffic. As a result, insider threats, malicious firmware updates, and maintenance interface compromises can be rapidly detected and appropriately mitigated. Please visit dersec.io to learn more about these detection and mitigation solutions.

Acknowledgements: We thank the security researchers for sharing their findings and the vendors for mitigating vulnerabilities described in this paper. To our knowledge, all reported vulnerabilities reported here have been resolved. With that said, new vulnerabilities will inevitably be revealed. When that occurs, responsible disclosure is essential to safely eliminate security weaknesses [26]. Details on how vulnerabilities should be reported must be provided by all organizations in this ecosystem.

Disclaimer: All 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 and given the opportunity to have their names redacted. Many of the companies included in the document expressed support for responsible disclosure practices and highlighted efforts they are taking to mature their solar energy cybersecurity programs.

Call To Action: Please share corrections, edits, and additions with Jay Johnson (security@dersec.io) for the next revision of this document.

Table 1: Chronological list of public solar cybersecurity attacks (orange) and vulnerability disclosures (blue).

#	Approx. Date	Product (Type)	Who	Attack or Vulnerability Details	Potential Access Level or 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	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
4	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
5	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
6	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
7	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
8	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 solar monitoring system.	CVE-2017-6048	R1
9	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
10	6/28/18	[redacted] Microinverter Gateway (Solar Monitor)	Knownsec	Sensitive information exposed via direct request to [redacted] URI. CVSS v3: 7.5.	Reconnaissance mechanism for [redacted] solar monitors: ZoomEye shows 258 online in Nov 2024; data leakage.	CVE-2018-12927	R1
11	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
12	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
13	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
14	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
15	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 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
16	1/23/20	[redacted] Inverters with Wi-Fi Dongles, e.g., [redacted] or [redacted] (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 single device when in range of the Wi-Fi network.		R1 R2 R3

17	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
18	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
19	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
20	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	
21	5/15/22	Contec SolarView Compact (Solar Monitor)	Ahmed Alroky - Alactive	Command injection via conf_mail.php in SolarView Compact v6.00. CVSS v3: 9.8.	Used by 30,000 PV sites total. 615 found exposed online with 425 of those running unpatched versions.	CVE-2022-29303	R1 R2 R3 R4
22	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
23	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
24	7/29/22	Inavitas Solar Log (Solar Monitor)	Unknown	SQL Injection vulnerability. CVSS v3: 9.8/9.4.	Unknown	CVE-2022-1277	R1
25	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
26	10/17/22	Kostal PIKO MP (Inverter)	David de Paula Santos	XSS via file upload feature.	Unknown	CVE-2022-42974	R1
27	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 R2 R3
28	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
29	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
30	4/15/23	[redacted] [redacted] (Cloud)	Anonymous	Unauthenticated user can create SuperAdministrator, with (a) permissions to read, delete, or modify any user account within [redacted], and (b) read, delete, or modify any plant within [redacted].	Full access to entire [redacted] fleet.		R1
31	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 injecton 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 total. 615 found online.	CVE-2023-27512 CVE-2023-27514 CVE-2023-27518 CVE-2023-27920 CVE-2023-27521	R1
32	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
33	6/27/23	Enphase Installer App (App)				CVE-2023-32274	
34	9/1/23	Hoymiles Microinverter HM-300 with DTU-Lite (Inverter); Hoymiles website (Cloud)	Sebastien (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
35	10/16/23	Growatt MIC600TL-X with ShineWIFI-X Stick (Inverter); Growatt Server (Cloud)	Sebastien (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

36	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
37	11/12/23	SolaX X1 Microinverter with SolaX Pocket WiFi 3.0 (Inverter); solaxcloud (Cloud)	Sebastien (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
38	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
39	12/27/23	[redacted] string inverter with [redacted] (Inverter); [redacted] (Cloud)	Sebastien (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
40	1/28/24	Growatt v8.1.0.0	l00neyhacker	Access sensitive information or execute injection attacks.	Potential cleartext downgrade attack.	CVE-2024-22678	R1
41	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
42	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
43	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
44	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
45	5/22/24	Deye Cloud/Website (Cloud)		Hard coded credentials; information leakage.			
46	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
47		Sunsynk Website (Cloud)					
48		Solax Website (Cloud)					
49		Growatt Website (Cloud)					
50		[redacted] Website (Cloud)					
51		Fox ESS Customer Website (Cloud)					
52	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.	Solar-Log1000 monitors up to 100 inverters with a total output of up to 1 MWp.	CVE-2024-40116 CVE-2024-40117	R1 R2
53	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
54	9/1/24	User credentials stolen for [redacted] (PV Monitoring Platform for the city of Kaunas, Lithuania)	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 representing hospitals and military academies.		R1