FORESCOUT

SUN:DOWN

Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems

FORESCOUT RESEARCH | VEDERE LABS

Threat Intelligence Sharing Partners

OT-ISAC Operational Technology Information Sharing and Analysis Center

ACSC Australian Cyber Security Centre

EE-ISAC

CISA Cybersecurity & Infrastructure Security Agency

Devices

- 19+ million monitored devices
- 39+ billion unique data points
- 6,500+ unique vendors
- 2,300+ unique OS versions

Threats

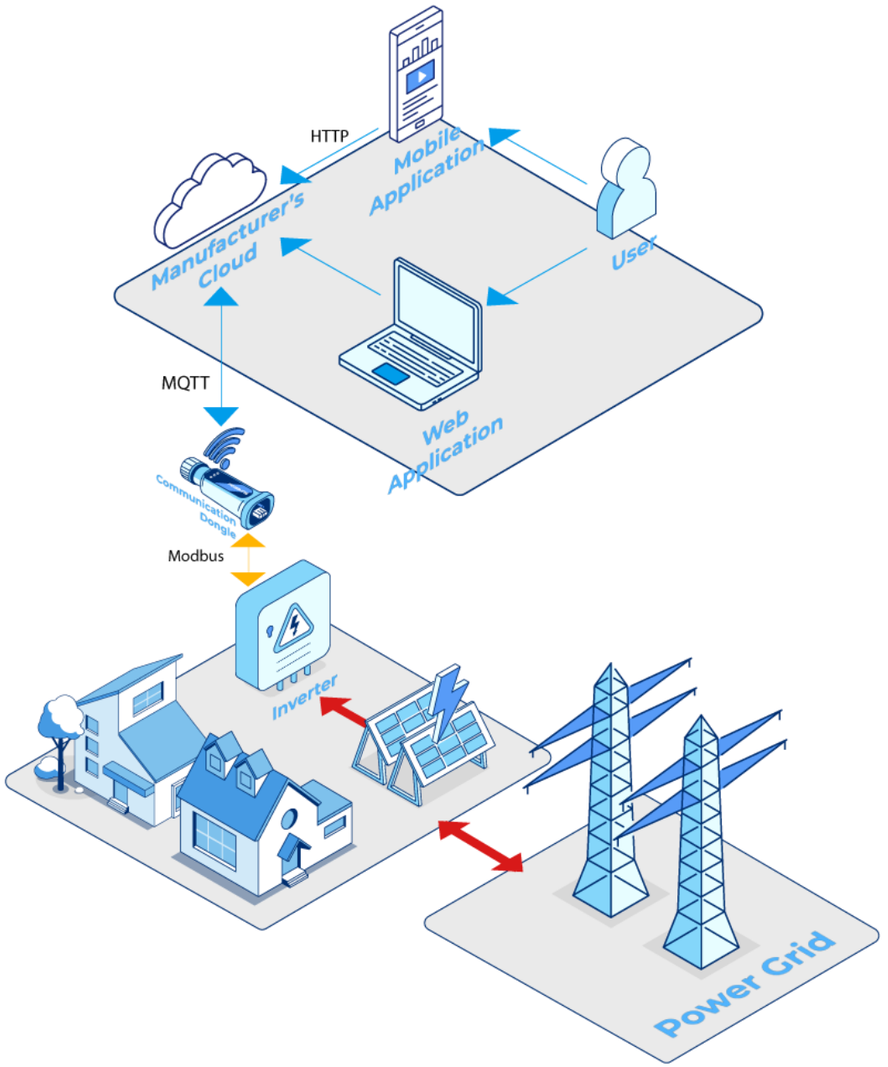
- 900+ million attacks
- 100,000+ malware samples
- 100+ ransomware group leak sites
- 20+ C2 types monitored on the Internet

Live data

forescout.vederelabs.com

Overview of Solar Power Systems

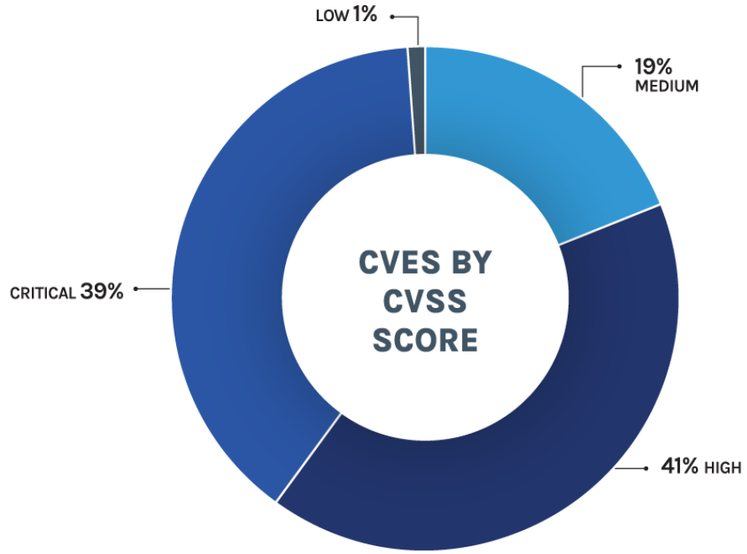
- Solar PV panels generate DC power, which is converted to AC by **inverters**
- These inverters are **grid-connected *and* cloud-connected IoT devices**
  - Enable remote monitoring and management
  - Sometimes require an extra dongle / data logger
- Large **attack surface**
  - Inverters (comm dongles) are not supposed to be accessible directly via the internet
  - However, they are managed via the **vendor's cloud, web apps and mobile apps**
  - Lots of other components we don't include in this talk: batteries, EV chargers, etc.



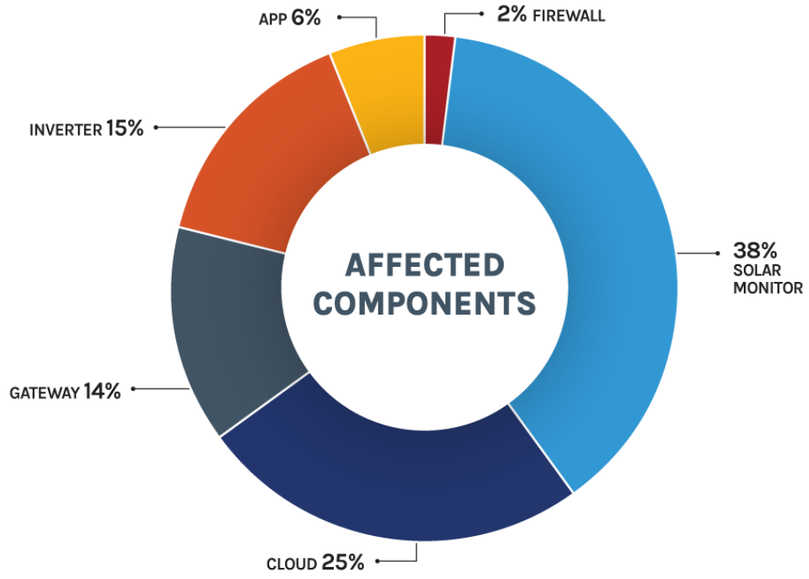
Previous Vulnerabilities

- Cataloged **93 previous vulnerabilities affecting 34 vendors**
  - CVEs since 2012, average of 10/year for the past 3 years
  - 80% high or critical CVSS
  - Most cases affected solar monitoring/cloud products
  - Relatively few issues found directly on the inverters
- Six vulnerabilities **regularly exploited by botnets since 2022**

Product	CVEs
CONTEC SolarView	CVE-2022-29303 CVE-2022-40881 CVE-2023-23333 CVE-2023-29919
APsytems	CVE-2023-28343
Altenergy	CVE-2024-11305



Source: Forescout Research Vedere Labs



Source: Forescout Research Vedere Labs

CVE catalog extended data from https://dersec.io/wp-content/uploads/2024/11/DERSec_Solar_Vulnerability_Summary_11-15-24.pdf

New Vulnerabilities

46 vulnerabilities in three vendors!

SMA

- **RCE** on cloud portal through **unrestricted file upload**

Potential control of an inverter fleet ?

GROWATT

- Lots of **Insecure Direct Object References (IDOR)**
- 2 x Stored XSS
- Broken authentication issues led to **data leakage** and **account takeover**

Potential control of a fleet?

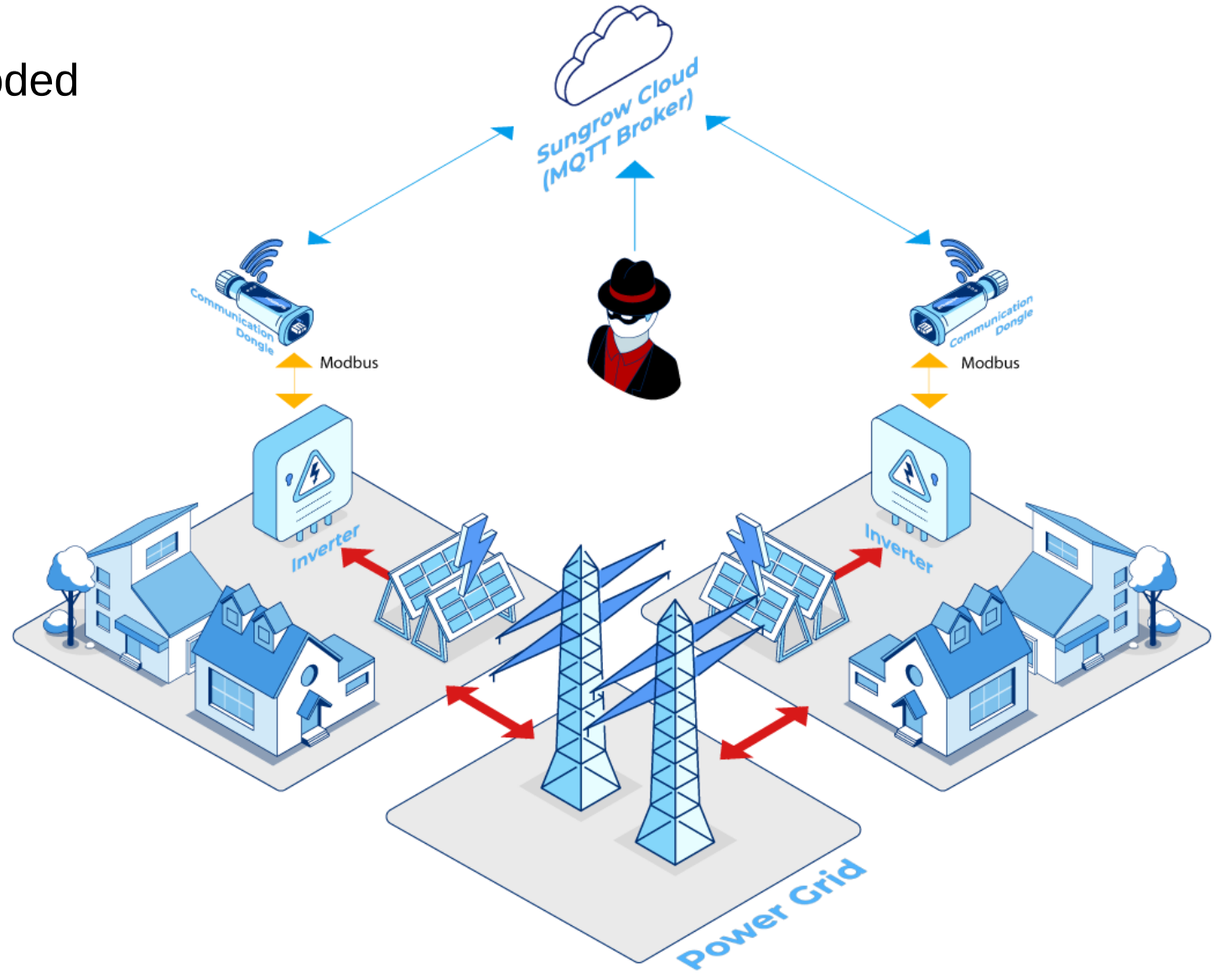
SUNGROW

- Again **many IDORs**
- Hardcoded credentials for MQTT
- Weak encryption in the mobile app communication
- Unsigned firmware update
- 4x **Buffer overflow** vulnerabilities in the inverter Dongle (WiNet-S), **one led to RCE**

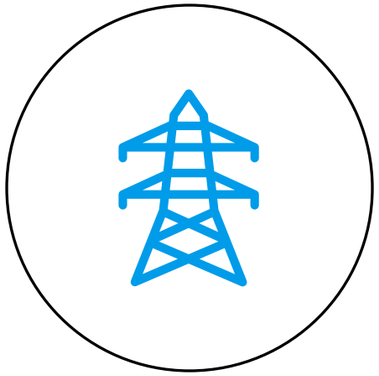
Potential control of a fleet?

Taking Control of Inverters

1. Harvest serial numbers via IDORs
2. Publish MQTT messages to the dongles via hard-coded credentials
3. Via the published messages, exploit an RCE on the dongles to gain control of inverters

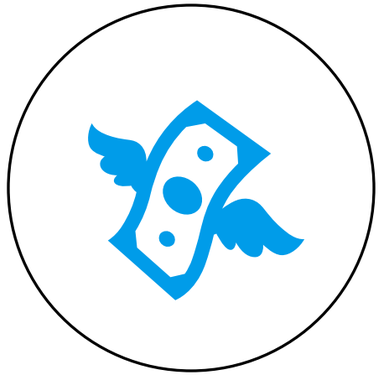


Impact



Grid Stability

- Control over many inverters allow attackers to target energy production
- If too many go down at the same time, it can cause grid stability issues



Financial Impact

- The same kind of control allows attackers to demand a ransom based on the threat to utilities

Recommendations

Manufacturers

Development

- **Devices:** holistic security architecture including secure boot, binary hardening, anti-exploitation features, permission separation etc
- **Applications:** proper authorization checks on web applications, mobile applications and cloud backends

Testing

- Regular penetration testing on applications and devices
- Consider bug bounty programs

Monitoring

Web Application Firewalls

Remember that a WAF does not protect against logical flaws

Users

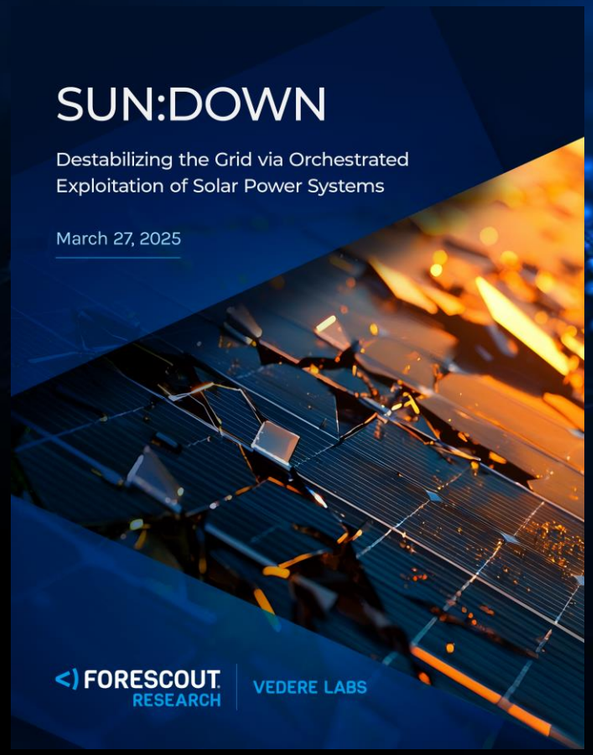
Residential and commercial users

- Change default passwords and credentials
- Use role-based access control
- Configure the recording of events in a log
- Update software regularly
- Backup system information
- Disable unused features
- Protect communication connections

Commercial and utility installations (in addition)

- Include security requirements into procurement considerations
- Conduct a risk assessment when setting up devices
- Ensure network visibility into solar power systems
- Segment these devices into their own sub-networks
- Monitor those network segments

Takeaways



- Solar power is growing massively and so is the attack surface
- Several components have vulnerabilities and they are starting to get targeted by opportunistic attackers
- There is potential for more targeted attacks that impact grid stability or utilities directly
- Risk mitigation depends on actions from users, installers, utilities, regulators and others
- The time to fix these problems is now!
- Read the full report on forescout.com/research

Thank you.

FORESCOUT

- Follow the research:
  forescout.com/research
- Subscribe to our threat feed:
  https://feeds.vederelabs.com
- Subscribe to our newsletter:
  forescout.com/research-labs/#newsletterslignup