### SolarView Compact Command Injection Vulnerability Industrial Control Systems hardware vulnerability exploited in the wild

CVEs: CVE-2022-40881, CVE-2022-29303

FortiGuard Labs observed a huge spike in attack attempts relating to a command injection vulnerability in SolarView Compact (Solar power

generation monitoring system) with upto more than 18,000+ unique IPS detections in the month of July 2023. The exploit works due to the vulnerability in SolarView Compact confi mail.php component, which fails to adequately sanitize the user-supplied input data, leading to command injection. Background SolarView Compact is a part of Solar energy monitoring solutions offered by CONTEC and SolarView Compact

**Announced** 

**Latest Developments** 

vendor website, particularly in the field of solar power generation, SolarView brand solutions are introduced at more than 30,000 power stations. If the SolarView Compact hardware is a part of a solar power generation site, the attacker may be able to exploit and affect loss of productivity and revenue and could also use it as a network pivot to attack other ICS resources.

specifically monitors and visualizes small to medium-scale solar power generation and storage. According to the

13 Dec, 2022: FortGuard Labs released IPS signature to detect and block attack attempts leveraging SolarView Compact Command Injection Vulnerability. (CVE-2022-40881, CVE-2022-29303)

23 March, 2023: FortiGuard Labs created an IPS signature to detect a different SolarView Compact Command Injection Vulnerability (CVE-2023-23333), however we do not see signs of it being exploited in the wild as of yet.

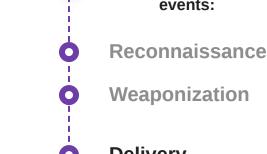
> 23333, however we recommend users to apply review patches and upgrade SolarView Compact devices if available and make sure the devices are protected and behind the IPS systems to mitigate any risks completely.

It is reported that all the vulnerabilties mentioned are fixed in SolarView Compact v8.0 and above.

FortiGuard customers remain protected by the IPS signatures for CVE-2022-40881, CVE-2022-29303, CVE-2023-

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity

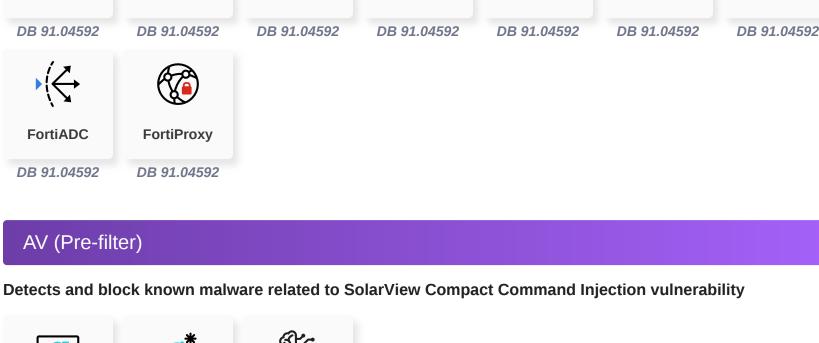
July 13, 2023: CISA added CVE-2022-29303 to its Known Exploited Catalog (KEV)



## Weaponization

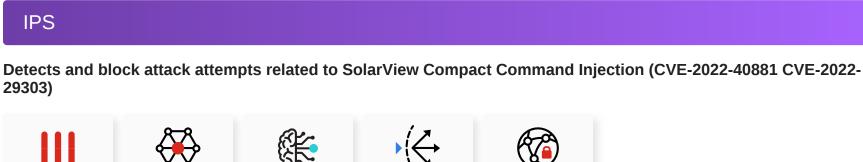
**Delivery** 

**FortiWeb FortiClient FortiSASE FortiMail FortiCASB** 



**FortiNDR** 

DB 91.04592



**Exploitation** 

**FortiNDR** 

DB 22.476

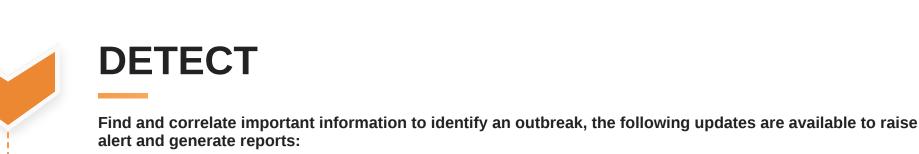


**FortiADC** 

DB 22.476

**FortiProxy** 

DB 22.476





**FortiSIEM** 

**FortiSOCaaS** 

**RESPOND** 

**Automated Response** 

# Response

(and recovery from) security incidents:



Improve security posture and processes by implementing security awareness and training, in preparation for

Train your network and security professionals and optimize your incident response to stay on top of the

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download

Experts to assist you with analysis, containment and response activities.

Develop containment techniques to mitigate impacts of security events:



and other forms of cyberattacks.

Attack Surface Hardening Check Security Fabric devices to build actionable configuration recommendations and key indicators.

**Business Reputation** Know attackers next move to protect against your business branding.

Security Rating

> FortiRecon: **EASM**

**Additional Resources Bleeping Computer** https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/ **Dark Reading** https://www.darkreading.com/ics-ot/3-critical-rce-bugs-threaten-industrial-solar-panels

Learn more about FortiGuard Outbreak Alerts

F#RTINET



**FortiCWP** 

**PROTECT** 

AV Detects and block known malware related to SolarView Compact Command Injection vulnerability

**FortiGate** 

**FortiEDR FortiSandbox** DB 91.04592 DB 91.04592

Behavior Detection Engine service detects unknown variants of the Mirai Malware **FortiSandbox** v4.0+

**Behavior Detection** 

**FortiGate** DB 22.476 **FortiSASE** 

DB 22.476

DB 1.00043

29303)

DB 0.00353

Installation C2 Action

IOC

**FortiAnalyzer** 

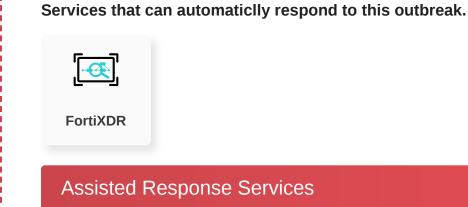
Outbreak Detection



**FortiAnalyzer** 

10 **FortiSIEM** 

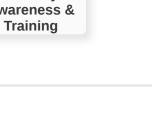
v6.5+



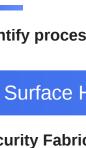
**RECOVER** 

**NOC/SOC Training** 

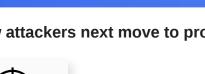
Response **NSE Training** Readiness **End-User Training** 















Identify processes and assets that need protection: