

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

Latest Developments

FortiGuard customers remain protected by the IPS signatures for CVE-2022-40881, CVE-2022-29303, CVE-2023-23333, 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 vulnerabilities mentioned are fixed in SolarView Compact v8.0 and above.

March 23, 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.

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

PROTECT

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


Reconnaissance

Weaponization


Delivery

AV


Detects known malware related to the Outbreak




FortiADC
DB 91.04592




FortiCASB
DB 91.04592




FortiCWP
DB 91.04592




FortiClient
DB 91.04592




FortiGate
DB 91.04592




FortiMail
DB 91.04592



FortiProxy
DB 91.04592



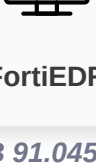
FortiSASE
DB 91.04592



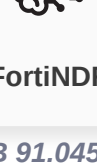
FortiWeb
DB 91.04592

AV (Pre-filter)

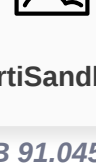
Detects known malware related to the Outbreak



FortiEDR
DB 91.04592



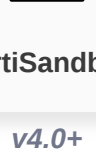
FortiNDR
DB 91.04592



FortiSandbox
DB 91.04592

Behavior Detection

Behavior Detection Engine service detects unknown variants of the Mirai Malware




FortiSandbox
v4.0+


Exploitation

IPS


Detects and blocks attack attempts leveraging the vulnerability




FortiADC
DB 22.476



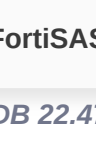
FortiGate
DB 22.476



FortiNDR
DB 22.476



FortiProxy
DB 22.476



FortiSASE
DB 22.476

Installation


C2

Action


DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:


IOC



FortiAnalyzer

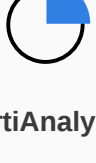


FortiSOCaaS



FortiSIEM

Outbreak Detection



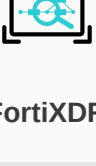
FortiAnalyzer
DB 2.00011

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

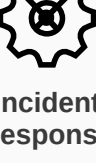
Services that can automatically respond to this outbreak.



FortiXDR

Assisted Response Services

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




Incident Response

RECOVER

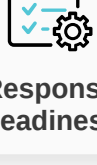
Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

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



NSE Training



Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.




Security Awareness & Training

IDENTIFY

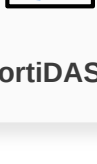
Identify processes and assets that need protection:

Attack Surface Hardening

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



Security Rating



FortiDAST

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](#)