

Solar container critical attack





Overview

Bitdefender identified several vulnerabilities in PV plant management platforms that could expose connected solar systems to remote access and manipulation. Nearly 35,000 solar power devices are remotely manageable and openly accessible to anyone from anywhere in the world, according to a new report from industrial cybersecurity firm Forescout. An attack on remote monitoring devices in Japan underscores an emerging cybersecurity threat to the rapidly growing solar component of the power grid. "There it goes," says Aditya K Sood as the remote dashboard for a solar power plant in. Since our first report in November 2024, we have cataloged an additional 50 CVE vulnerabilities in solar-based Distributed Energy Resource (DER) systems. Cyble researchers scanned web for solar PV devices and found over 134,000 products from various vendors accessible.



Solar container critical attack



SolarWinds Compromise, Campaign C0024 , MITRE ATT& CK®

The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious ...

Exporting Solar Solutions: Critical Technical Standards

To successfully export solar solutions to global markets, manufacturers must adhere to three primary tiers of certification: International Electrotechnical Commission (IEC) standards for ...



Hijack of monitoring devices highlights cyber threat to solar power

An attack on remote monitoring devices in Japan underscores an emerging cybersecurity threat to the rapidly growing solar component of the power grid.

How hackers capture your solar panels and cause grid havoc

In September 2024, a cyberattack against a solar park in Lithuania was carried out which US-based cybersecurity firm Cybel linked to hacking groups affiliated with Russia.



How to Survive a Nuclear Attack: Complete Survival Guide , Defcon ...

What to do if there's a nuclear attack. Complete survival guide covering immediate actions, sheltering, radiation protection, and long-term survival.

Understanding and Responding to the SolarWinds Supply Chain Attack...

Russia conducted the most damaging cyber attack in history, NotPetya, by inserting malicious code into a seemingly routine update for Ukrainian accounting software, starting a global ...



Vast array of solar power equipment left exposed online

Nearly 35,000 solar power devices are remotely manageable and openly accessible to anyone from anywhere in the world, according to a new report from industrial cybersecurity firm ...





Salt Typhoon

In November 2025, Australian Security Intelligence Organisation director-general Mike Burgess said hackers linked to the Chinese government and military had attempted to access Australia's critical ...



Contact Us

For catalog requests, pricing, or partnerships, please visit:
<https://goodstays.co.za>