What to do if the inverter of the communication base station is hijacked

Title: What to do if the inverter of the communication base station is hijacked
Generated on: 2026-03-24 04:22:10

Over the past nine months, forensic security teams have logged multiple brands of Chinese solar inverters containing hidden wireless communication equipment. Investigators have ...

Growatt inverters can be hijacked via the cloud backend by listing usernames from an exposed Growatt API, and then use these usernames for account-takeover through two IDOR ...

Detecting rogue base stations is a complex but essential task in maintaining the security and privacy of mobile communications. By combining technological solutions with proactive ...

Fake base stations, or IMSI catchers, are increasingly used by state and criminal actors to spy, disrupt, or impersonate mobile users. This blog explores how they work, who deploys them, ...

Inverters are the interface between solar panels and the grid. If the inverter"s software isn"t updated and secure, its data could be intercepted and manipulated. An attacker could also embed code in an ...

This investigative article exposes the discovery of undocumented communication devices hidden in Chinese-made solar inverters, creating unprecedented vulnerabilities in global power grids.

Experts uncover rogue devices in Chinese-made inverters and batteries, prompting U.S. and EU nations to review renewable tech security.

Inverters are highly digitized products, often referred to as the "heart" or "brain" of a photovoltaic system. In theory, whoever could control the inverter could remotely interrupt or ...

Website: https://www.studioogrody.com.pl