‘Rogue’ communication devices found on Chinese-made solar power inverters

The devices could give adversaries a way to disable power grids, damage energy infrastructure and trigger blackouts, specialists say.

U.S. officials have discovered undisclosed communication devices on the power inverters of some Chinese-manufactured solar panels, Reuters reported today based on anonymous sources within the federal government.

The inverters are part of the hardware package connecting solar arrays to the power grid. The package includes communication devices so technicians can monitor performance and have remote access for maintenance. These devices are disclosed in what’s called a software bill of materials – a listing of the components that comprise the package. The communication devices uncovered by the government are considered rogue because they’re undisclosed.

These devices “provide additional, undocumented communication channels that could allow firewalls to be circumvented remotely, with potentially catastrophic consequences,” Reuters reported the sources as saying.

Inverters are also included in other types of energy hardware, including batteries and heat pumps, and officials have found undisclosed devices in some of those as well.

“Over the past nine months, undocumented communication devices, including cellular radios, have … been found in some batteries from multiple Chinese suppliers,” the report said.

Security risk

Chinese companies are the biggest manufacturers of power inverters, used by manufacturers of solar panels, wind turbines and other types of renewable power components around the world.

The devices raise security concerns because Chinese companies are required by law to cooperate with their government’s intelligence agencies, giving those agencies control over Chinese-made inverters that connect to foreign grids, security experts told Reuters.

That could enable the Chinese government to skirt firewalls and switch off the inverters remotely, or change their settings, destabilizing power grids, damaging energy infrastructure and triggering blackouts, the Reuters report said.
“That effectively means there is a built-in way to physically destroy the grid,” one of the unnamed sources told Reuters.

One such incident occurred in November, when solar power inverters in the U.S. and elsewhere were disabled from China, highlighting the risk of foreign influence over local electricity supplies, sources told Reuters.

A spokesperson for the Chinese government pushed back against the accusation it would use the devices to cause disruption to power grids.

“We oppose the generalisation of the concept of national security, distorting and smearing China’s infrastructure achievements,” the spokesperson told Reuters.

Stepped-up restrictions

Congress has been concerned for years with the security issues posed by China’s dominance in strategic infrastructure manufacturing. Earlier this year, Sens. Rick Scott, R-Fla., and Maggie Hassan, D-N.H., introduced the Decoupling from Foreign Adversarial Battery Dependence Act, which would prohibit the Department of Homeland Security from purchasing batteries from some Chinese entities.

“With our nation currently sourcing a majority of its batteries from Chinese-linked manufacturers, we’re subject to a major, unnecessary risk to our national security,” Scott said when the bill was introduced.

There’s no similar bill to restrict Chinese-made inverters but some administrative restrictions are in place. Starting in 2019, the federal government began imposing prohibitions on the use of inverters and other infrastructure equipment manufactured by Huawei Technologies, the largest maker of the devices. Other efforts are underway to reduce the reliance on Chinese equipment, a spokesperson for the U.S. Department of Energy told Reuters.

“As more domestic manufacturing takes hold, DOE is working across the federal government … to integrate trusted equipment into the power grid,” the spokesperson said.