Issued 8/9/17

Hackers Could Exploit Solar Power Equipment Flaws to Cripple Green Grids

A Dutch researcher says he found a way to cause mischief on power grids by exploiting software bugs in solar power systems. Specifically, Willem Westerhof, a cybersecurity researcher at ITsec, said he uncovered worrying flaws within power inverters – the electrical gear turns direct current from solar panels into alternating current that can be fed into national grids.

These vulnerabilities could be exploited remotely if the equipment was connected to a network accessible to an attacker, it is claimed: a hacker on the same LAN, or reaching an internet-facing inverter from the other side of the world, could get busy abusing the bugs to control the amount of juice going out onto the grid. Westerhof said he discovered 21 vulnerabilities in inverters manufactured by German specialists SMA Solar Technology, which sells more than $1bn of kit every year.

Since at its daily power generation peak, solar accounts for almost half of Germany's energy production, an inverter hack would have serious consequences. "In Europe there is over 90 GW of [photovoltaic] power installed. An attacker capable of controlling the flow of power from a large number of these devices could therefore cause peaks or dips of several GigaWatts, causing massive balancing issues which may lead to large-scale power outages," he said. The attack scenario – which Westerhof named Horus after the Egyptian god of the sun – would

involve hackers subverting a large number of inverters. He argues these could be hijacked and programmed to either (a) Flood power onto the grid, causing other generators to shut down to prevent the network overloading, or (b) Underpower the grid to cause brownouts or blackouts. Causing massive fluctuations – gigawatts-worth – in power generation in a very short time period would be rather irritating if done at peak solar panel generating time. He cited the 2015 solar eclipse over Germany, which caused a massive drop-off in power generation. Because this happened at a predictable time, the solar slump was manageable. But an attack at random moments and high speed would cause major problems.

After examining SMA's inverters, Westerhof contacted the manufacturer in December with his findings, following responsible disclosure best practices. However, he ran into a morass of buck-passing over fixing the issue, which is why the publication of his research was delayed to this month.