US energy department and other agencies hit by hackers in Movelt breach

Publication Date: 2023-06-16

Author: Unknown

Section: Technology

Tags: Hacking, news

Article URL: https://www.theguardian.com/technology/2023/jun/16/moveit-transfer-hack-department-of-energy

The US Department of Energy and several other government agencies were hit in a global hacking campaign that exploited a vulnerability in widely used file-transfer software, officials said this week. Data was “compromised” at two entities within the energy department when hackers – attributed to a Russia-linked criminal gang – gained access through a security flaw in Movelt Transfer, the department said in a statement on Thursday. The British energy giant Shell and the University System of Georgia, the Johns Hopkins University and the Johns Hopkins Health System were also hit, all three groups said in separate statements. The latest victims add to a growing list of hacks on other US and international entities that also targeted the Movelt software. Known victims to date include Louisiana’s Office of Motor Vehicles, Oregon’s transport department, the Nova Scotia provincial government, British Airways, the BBC and the UK drugstore chain Boots. Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (Cisa), told reporters that unlike the meticulous, stealthy SolarWinds hacking campaign attributed to state-backed Russian intelligence agents that was months in the making, this campaign was short, relatively superficial and caught quickly. “Based on discussions we have had with industry partners … these intrusions are not being leveraged to gain broader access, to gain persistence into targeted systems, or to steal specific high-value information – in sum, as we understand it, this attack is largely an opportunistic one,” Easterly said. “Although we are very concerned about this campaign and working on it with urgency, this is not a campaign like SolarWinds that presents a systemic risk to our national security or our nation’s networks,” she added. A senior Cisa official said neither the US military nor intelligence community was affected. An energy department spokesperson, Chad Smith, said two agency entities were compromised but did not provide more detail. Louisiana officials said on Thursday that people with a driver’s license or vehicle registration in the state probably had their personal information exposed. That included their name, address, social security number and birthdate. They encouraged Louisiana residents to freeze their credit to guard against identity theft. The Oregon transport department confirmed on Thursday that the attackers accessed personal information, some sensitive, for about 3.5 million people to whom the state issued identity cards or driver’s licenses. Cl0p, the Russian-linked ransomware syndicate behind the hack, announced last week on its dark web site that its victims, who it suggested numbered in the hundreds, had until Wednesday to get in touch to negotiate a ransom or risk having sensitive stolen data dumped online. The gang, among the world’s most prolific cybercrime syndicates, also claimed it would delete any data stolen from governments, cities and police departments. US officials “have no evidence to suggest coordination between Cl0p and the Russian government”, the official said. Movelt Transfer is a popular tool used by organizations to share sensitive information with partners or customers. Hackers took advantage of a security flaw that its maker,

Progress Software, discovered late last month and issued a patch. A MoveIt spokesperson said the company had “engaged with federal law enforcement” and was working with customers to help them apply fixes to their systems. But cybersecurity researchers say scores if not hundreds of companies could by then have had sensitive data quietly exfiltrated. “At this point, we are seeing industry estimates of several hundred of victims across the country,” the senior Cisa official said.