Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

01 July 2024

PIN Number

20240701-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP: CLEAR**

Please contact the FBI with any questions related to this Private Industry Notification via your local Cyber Squad.

www.fbi.gov/contact-us/field-offices

Expansion of US Renewable Energy Industry Increases Risk of Targeting by Malicious Cyber Actors

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification (PIN) to highlight how malicious cyber actors may seek to disrupt power generating operations, steal intellectual property, or ransom information critical for normal functionality to advance geopolitical motives or financial gain within the US renewable energy industry. With federal and local legislature advocating for renewable energies, the industry will expand to keep pace, providing more opportunities and targets for malicious cyber actors.

Historical Cyber Incident Involving the Renewable Energy Industry's Operations

In 2019, a private company, which operates solar assets in the United States, lost visibility into approximately 500 MW of its wind and photovoltaic sites in California, Utah, and Wyoming as a result of a denial-of-service attack that exploited an unpatched firewall. While it was unclear if this specific incident was a deliberate cyberattack targeting this specific company, the incident highlighted the risks posed by a security posture that relies on outdated software.

Risks Associated with a Cyber Incident Impacting Solar Infrastructure

A cyber attack against a solar panel system—residential or commercial—would likely focus on targeting the system's operational technology (OT) software and hardware; specifically, malicious cyber actors could attempt to gain control over a solar panel system through the inverters. Inverters are responsible from converting the direct current (DC) energy that the solar panels generate into practical alternating current (AC) electricity. Some inverters have built-in monitoring systems that connect to the Internet, which increases their risk profile; if a malicious cyber actor took control of a residential inverter, they could attempt to reduce that solar panel system's power output or target that home's battery storage inverter (if one is onsite) to overheat it.

While cyber attacks against residential solar infrastructure have been rare historically, malicious cyber actors could seek to target microgrids, which local power systems use to operate independently of the larger electrical grid during a power outage. To attain a larger disruption, malicious cyber actors could attempt to target inverters at solar farms; however, researchers are working to counter this potential risk through a passive sensor device that can detect unusual activity in the electrical current.

Threat

Structural shifts in the reduced cost of implementation of renewable energy and incentives for development of clean energy have created new targets and opportunities for cyber threat actors to disrupt and exploit for their own gain.

- The Inflation Reduction Act's passage signaled a new push by the federal government to encourage renewable energy options for different US municipalities and expand these technologies to more US citizens. As renewable energy, which generates about 21% of all US electricity as of late 2023, becomes more nationally prevalent, US consumers are increasingly exploring ways to reduce their own fossil fuel consumption through new government tax incentives. This has included US federal agencies, such as the DoD, which is the largest consumer of energy in the US government, much of which it sources from local electric grids.

- In late 2023, the Metropolitan Washington Council of Government set a non-binding goal for the region to install 250,000 solar rooftops by 2030. In 2019, Virginia established the following three objectives concerning its statewide energy production: first, by 2028, Virginia will achieve 5,500 MW of wind and solar energy (of which 3,000 MW should be under development by 2022); by 2030, renewable energy will power 30 percent of Virginia's electric system; and finally, by 2050, carbon-free energy sources—wind, solar, and nuclear energy—will power 100 percent of Virginia's electricity.

Recommendations

The FBI recommends organizations take the steps below to improve their organization's security posture in response to these new activity trends. The FBI recommends organizations establish and maintain strong liaison relationships with the FBI Field Office in their region. The location and contact information for FBI Field Offices can be located at www.fbi.gov/contact-us/field-offices. Through these partnerships, the FBI can assist with identifying vulnerabilities and mitigating potential threat activity. The FBI further recommends organizations review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident.

The FBI encourages current and former employees of companies within the renewable industry to report cyber intrusions targeting either themselves or their organization, as well suspected elicitation attempts by foreign nationals outside of the organization. Private industry partners can contact their local FBI office to report security concerns and request threat briefings. Partners in the renewable energy industry can address espionage and cyber threats by:

- Routinely monitor network activity for unusual or suspicious traffic and activity;
- Update company networks to patch any potential security vulnerabilities, along with firewalls and antivirus software;
- Report computer network intrusions to the appropriate law enforcement organizations;
- Report unexpected visits to company facilities or suspicious solicitations to employees while attending conferences or during foreign travel to law enforcement.
- Consider risks from vendors (to include sub-vendors or parent companies) carefully to avoid exposure to deliberate exploitation of supply chain vulnerabilities as an attack vector; this includes scrutinizing vendors from nation-states associated with cyberattacks or those subject to national legislation requiring them to hand over data to foreign intelligence services

The FBI and recommends network defenders apply the following general mitigations to limit potential adversarial use of common system and network discovery techniques.

Preparing for Cyber Incidents –

- **Maintain offline backups of data**, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and that backup data will be accessible when it is needed.

- **Ensure all backup data is encrypted, immutable** (that is, cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.

- **Review the security posture of third-party vendors and those interconnected with your organization.** Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

- **Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs** under an established security policy.
- **Document and monitor external remote connections.** Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).

Identity and Access Management –

- **Require all accounts** with password logins (for example, service account, admin accounts, and domain admin accounts) **to comply** with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
    - Store passwords in hashed format using industry-recognized password managers;
    - Add password user "salts" to shared login credentials;
    - Avoid reusing passwords;
    - Implement multiple failed login attempt account lockouts;
    - Disable password "hints";
    - Refrain from requiring password changes more frequently than once per year unless a password is known or suspected to be compromised. **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed

and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Secure and closely monitor** remote desktop protocol (RDP) use.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.

Vulnerability and Configuration Management –

- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.
- **Disable unused ports.**
- **Consider adding an email banner to emails** received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Disable command-line and scripting activities and permissions**. Privilege escalation and lateral movement often depend on software utilities running from the command line. If

threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.

- **Ensure proper device configuration and that security features are enabled**.
- **Disable ports and protocols not actively used** for a business purpose (such as RDP Transmission Control Protocol Port 3389).

Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB (such as SMB version 1). Threat actors use SMB to propagate malware across organizations.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or ic3.gov. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP: CLEAR**. The information in this product may be shared with peers and partner organizations within your sector or community, but not via publicly accessible channels.