March 29, 2022
Rev. April 27, 2022

Mitigating Attacks Against Uninterruptible Power Supply Devices

Act Now
Mitigate attacks against UPS devices by immediately removing management interfaces from the internet.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy are aware of threat actors gaining access to a variety of internet-connected uninterruptible power supply (UPS) devices, often through unchanged default usernames and passwords.

In recent years, UPS vendors have added Internet of Things capability, and UPSs are routinely attached to networks for power monitoring, routine maintenance, and/or convenience.

UPS devices provide clean and emergency power in a variety of applications when normal input power sources are lost. Organizations operating industrial operational technology and control systems environments also use UPS devices for a variety of other applications.[1] Loads for UPSs can range from small (e.g., a few servers) to large (e.g., a building) to massive (e.g., a data center). Various different groups within an organization could have responsibility for UPSs, including but not limited to IT, building operations, industrial maintenance, or even third-party contract monitoring service vendors.

RECOMMENDED ACTIONS

- **Immediately enumerate all UPSs and similar systems and ensure they are not accessible from the internet.** In the rare situation where a UPS device or similar system's management interface must be accessible from the internet, ensure that compensating controls, such as the following, are in place, including:
  - Ensure the device or system is behind a virtual private network.
  - Enforce multifactor authentication.
  - Use strong, long passwords or passphrases in accordance with National Institute of Standards and Technology guidelines (for a humorous explanation of password strength, see XKCD 936).
- Check if your UPS's username/password is still set to the factory default. If it is, update your UPS username/password so that it no longer matches the default. This ensures that going forward, threat actors cannot use their knowledge of default passwords to access your UPS. Your vendor may provide additional guidance on changing default credentials and/or additional recommended practices.
- Ensure that credentials for all UPSs and similar systems adhere to strong password length requirements and adopt login timeout/lockout features.

INCIDENT RESPONSE

If your organization is impacted by an incident or suspected incident:

- Implement your cyber incident response plan. See CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks for incident response practices and operational procedures.
- Follow guidance on technical approaches to uncovering and remediating malicious activity for incident response best practices in the joint Cybersecurity Advisory by CISA and the cybersecurity authorities of Australia, Canada,

[1] Examples include rail and light rail remote switch house and positive train control systems; healthcare critical care unit equipment (e.g., heart monitors, air supplies); maritime naval communications, bilge pumps, and rudder systems; emergency services such as traffic light switch houses; energy substations controlled via supervisory control and data acquisition and switching and relay systems; and water and wastewater bilge pumps and flow control systems.

New Zealand, and the United Kingdom.

- Report incidents or anomalous activity immediately to CISA's 24/7 Operations Center at report@cisa.gov or 888-282-0870.

ADDITIONAL RESOURCES

- See CISA's Shields Up webpage for additional actions to take now to defend against malicious cyberactivity.
- Refer to CISA's Cyber Essentials for additional recommendations on managing cybersecurity risks.
- See Questions Every CEO Should Ask About Cyber Risks for additional best practices to help companies understand their risks and prepare for cyber threats.
- See Cybersecurity Advisory: NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems for more guidance specific to organizations supporting U.S. critical infrastructure.
- See CISA's Cyber Resource Hub webpage for more information on CISA's no-cost assessments to help organizations evaluate their operational resilience and cybersecurity practices.