HC3: Alert

March 30, 2022 TLP: WHITE Report: 202203301500

Mitigating Attacks Against Uninterruptible Power Supply Devices

Executive Summary

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 an Internet of Things (IoT) capability, and UPSs are routinely attached to networks for power monitoring, routine maintenance, and/or convenience.

Report

CISA Insight - Mitigating Attacks Against Uninterruptible Power Supply Devices
Mitigating Attacks Against Uninterruptible Power Supply Devices (cisa.gov)

Impact to HPH Sector

UPS devices can be found in all sectors and provide clean and emergency power in a variety of applications when normal input power sources are lost. 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). 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.

Among CISA's recommendations are the following:

- Mitigate attacks against UPS devices by immediately removing management interfaces from the internet.
- Immediately enumerate all UPSs and similar systems and ensure they are not accessible from the internet
- Check if your UPS's username/password is still set to the factory default.
- Ensure that credentials for all UPSs and similar systems adhere to strong password length requirements

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors. All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.

References

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback