National Cyber Security Centre

2203292028-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Targeting of Uninterruptible Power Supply Devices (UPS)

2022-03-30

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

The US Cybersecurity and Infrastructure Security Agency (CISA) has released an alert regarding the targeting of Uninterruptible Power Supply (UPS) devices by malicious actors. UPS devices offer emergency backup power in many organisations.

Many UPS devices have Ethernet connections and in some cases are connected directly to the Internet. These Internet-facing UPS systems are particularly vulnerable to attack as quite often default usernames and passwords remain unchanged, offering malicious actors opportunities to remotely access these devices.

Impact

Malicious actors may take control of UPS devices to disable or catastrophically destroy functionality, or power down connected ICT equipment. Emergency power for critical systems would then not be available which can lead to operation disruption.

Recommendations

The NCSC recommends that affected organisations review the CISA Advisory, adhere to the actions recommended below, and if required ensure service providers take necessary measures:

- Immediately enumerate all UPS devices and similar systems and ensure they are not accessible from the internet. In the rare situation where a UPS device or similar systems' management interface must be accessible from the Internet, ensure that compensating controls are in place, including:
  - Ensure the device or system is only accessible using a virtual private network
  - Enforce multi-factor authentication (MFA)
  - Use strong, long passwords or passphrases
  - Consider your need to access and monitor UPS devices while facing disruption to power-supply.
- Check if your UPS's username/password is still set to the factory default. If so, 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 UPS devices and similar systems adhere to strong password length requirements and adopt login timeout/lockout features.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie