Cybersecurity Vulnerability Disclosure

Overview

Attackers can easily identify and access Internet-connected systems that use default passwords. It is imperative that users change default manufacturer passwords and restrict network access to critical and important systems.

The United States Computer Emergency Readiness Team (US-CERT) has issued Alert (TA13-175A) “Risks of Default Passwords on the Internet:

http://www.us-cert.gov/ncas/alerts/TA13-175A.

Vulnerability Overview

Factory default software configurations for embedded systems, devices, and appliances often include simple, publicly documented passwords. These systems usually do not provide a full operating system interface for user management, and the default passwords are typically identical (shared) among all systems from a vendor or within product lines. Default passwords are intended for initial testing, installation, and commissioning. Most vendors recommend changing the default password before deploying the system in a production environment however this may not have been implemented in all situations.

What is the risk? Attackers can easily obtain default passwords and identify Internet-connected systems. Passwords can be found in product documentation and compiled lists are available on the Internet. It is feasible to scan the entire IPv4 Internet, making it possible to identify and exploit exposed systems using search engines like Shodan (www.shodanhq.com).

Product(s) Affected

If an IP-enabled controller or embedded device is in operation at a site using a default password; the device may be at risk.

Mitigation

Change the default password for built-in user accounts. Please refer to the respective product document for instructions on how to change user account passwords.

It is also recommended that passwords be routinely changed, when permitted by the product, following these rules:

- Passwords should not be common words or names
- Passwords should include at least one alphanumeric, one upper case, one lower case, and one special character

Schneider Electric recommends confirming each device has this important security measure in place as part of a special or planned service of each site. Immediate action is recommended for all devices using default passwords.

Where devices have limited or no opportunity to modify the Login/Password combination, or when there is significant risk to changing the default password, protecting the device from exposure to untrusted networks is even more important. The best mitigation in this case is to ensure the device isn't directly connected to an untrusted network such as the Internet. Installing firewalls to block traffic and Intrusion Detection Systems to monitor for unusual message patterns can reduce risk and provides security measures for such devices if disconnection is not an option.

For More Information

This document is intended to help provide an overview of an identified vulnerability and actions required to mitigate it. To obtain full details on this issue and assistance with protecting your installation, please contact your local Schneider Electric representative. These organizations are aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com