Cybersecurity Vulnerability Disclosure

Overview

Schneider Electric has been notified by ICS-CERT (http://www.us-cert.gov/control_systems/ics-cert/) of security vulnerabilities that exist within the TAC I/A Series G3 product line.

Vulnerability Overview

The vulnerabilities identified include a directory traversal, weak credential storage, session cookie weaknesses, and predictable session IDs, all of which can be exploited remotely depending on the installation environment.   Successful exploitation of these vulnerabilities will lead to potential data leakages and possible privilege escalation.

Product(s) Affected

Products susceptible to these vulnerabilities include all current versions of the I/A Series G3 software.

Vulnerability Details

- Directory traversal - By default, the I/A G3 software is not configured to deny access to restricted parent directories.
- Weak credential storage - The system insecurely stores user authentication credentials, which are susceptible to interception and retrieval.
- Cookie weaknesses - Usernames and passwords are stored using Base64 encoding in a cookie within the default authentication configuration.
- Predictable session IDs - The software generates a predictable session ID or key value.

Mitigation

Schneider Electric strongly recommends all I/A Series G3 users upgrade to the latest version appropriate maintenance build (3.5.39 or 3.6.47) and apply the patch to correct this vulnerability.

Customers with I/A Series G3 systems older than 3.5 are strongly encouraged to upgrade to the latest version of the I/A Series G3 software to take advantage of the latest security features.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric Buildings Business representative. These organizations will be fully aware of the situation and can support you through the process.

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