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 vulnerability identified is a directory traversal.

Product(s) Affected

Products susceptible to this vulnerability include I/A Series G3 v3.5 and v3.6 software.

Vulnerability Details

- Directory traversal - allows a user with a valid user account or guest privileges to escalate their privileges.

Mitigation

Schneider Electric strongly recommends all I/A Series G3 users upgrade to the latest version appropriate maintenance build (3.5.39, 3.5.403, 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 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