REMEDIATION ACTIONS FOLLOWING THE INCIDENT ON CHIYU SENSORS DEPLOYED BY SOLAR-OT

Deployment of the updated version of the firmware & Hardening of the SOLAR-OT platform

Author	Validated by
Deirdre STARSKY, Technical project manager	Elena PIZARI, Industrial Director

OBJECTIVE

This document specifies the 2 remediation actions following the incident on the access control systems deployed by SOLAR-OT:

1. The emergency deployment of the firmware update on all systems
2. The hardening of the monitoring platform

1. EMERGENCY DEPLOYMENT OF THE FIRMWARE UPDATE

The CHIYU manufacturer has developed an update of the firmware of the 'SEMAC' access control system mitigating the vulnerability => it must be deployed urgently by SOLAR-OT on all sites

Here is the version number of the firmware to deploy on all SEMAC S2 devices (67% of the park): 670VYJLN
Here is the version number of the firmware to deploy on all SEMAC S3V3 devices (33% of the park): 628AUYSD

2. HARDENING OF THE SOLAR-OT PLATFORM

CONFIGURATION

The objective is to limit the technical elements that can be used to carry out an attack, by installing only the essential services and equipment.

The reinforcement of the security level is achieved by :

- Limiting platform's functions
- Control of the platform's hardware elements

A. Modify By-default settings

Each component is reconfigured according to standards, including

- Technical accounts and associated authentication elements
- The network ports used
- Installation and working directories
- Access rights on directories and files
- The account used to run a service or a process, and the rights associated to this account
- The configuration files of the security elements, in particular traceability.

B. Restricting accessible functions

Only modules essential to operations and security of SOLAR-OT platform are maintained and are subject to accurate configuration, regular maintenance and supervision.

For this purpose, the operator analyzes the technical functions of the platform to exclude services or features installed but not used.

Each hardware or software configuration is inventoried in the form of a reference configuration.

C. Connected elements inventory

The operator proceeds to a complete technical inventory of the elements constituting the platform and maps them. The inventory includes the equipment that can connect to the platform permanently or temporarily, physically or remotely (workstation, server, peripheral...).

In the case where a third party connects to the platform, the operator notes it in his mapping and takes it into account in the risk analysis.

D. Use of managed elements

The operator manages every elements directly, including:

- Deployment of updates
- Administration of elements
- Remote configuration

PARTITIONING

The platform follows a segmentation logic by restricting each subsystem to its own actions in order to

- Contain an attack
- Limit compromise impact
- Adapt the security level of each sub-system

Partitioning applies to both physical and logical resources.

A. Subsystem segmentation

The segmentation into subsystems is done according to the following criteria:

- Functionality
- Level of data protection
- Level of exposure
- Level of security

Any connection between subsystems must be justified by a functional need.

B. Physical partitioning

There is a dedicated server to most critical applications.

C. Logical partitioning

Every data stored on the server is encrypted. Each subsystem follows its own encryption mechanism.

All communication between subsystems is carried out through the encrypted and authenticated virtual private network.

REMOTE ACCESS

A. Public access

Public access follows the HTTPS protocol and the platform is authenticated by presenting a server certificate.

Two-factor authentication is implemented for the platform's users.

B. Nomad access

The mobile workstations are configured to establish an authenticated and encrypted tunnel to the platform. The tunnel cannot be disabled, and access to the Internet or a local network is impossible.

The system partition and the data partition are fully encrypted

Two-factor authentication is in place on the workstation.

NETWORK FILTERING

In addition to the partitioning, filtering mechanisms are implemented.

A. Filtering points

The interconnections between subsystems are the main filtering points to which perimeter and local filtering are applied.

B. Filtering rules

The global flow matrix includes the filtering rules in force. It is updated annually.

C. Implementation

Filtering is ensured by dedicated firewalls based on the principle of authorization lists.