ACCIONES DE REMEDIACIÓN TRAS EL INCIDENTE CON LOS SENSORES CHIYU DESARROLLADOS POR SOLAR-OT

Implementación de la última versión de firmwares & Endurecimiento de la plataforma de supervisión SOLAR-OT

Autor	Validado por
Deirdre STARSKY, Jefa de Proyectos Técnicos	Elena PIZARI, Directora General de Industria

OBJETIVO

Este documento especifica las 2 acciones de remediación que deben llevarse a cabo tras el incidente con los sistemas de control de acceso desarrollados por SOLAR-OT:

1. Despliegue urgente de la actualización del firmware en todos los sistemas
2. Refuerzo de la configuración de la plataforma de supervisión

1. DESPLIEGUE URGENTE DE LA ACTUALIZACION DEL FIRMWARE

El fabricante CHIYU ha desarrollado una actualización de firmware para los sistemas de control de acceso 'SEMAC' que corrige la vulnerabilidad => SOLAR-OT debe implementarlo de manera urgente en todos los sitios

Este es el número de versión del firmware que debe implementarse en los SEMAC S2 (67 % del parque): 670VYJLN
Este es el número de versión del firmware que debe implementarse en los SEMAC S3V3 (33 % del parque): 628AUYSD

2. REFUERZO DE LA CONFIGURACIÓN DE LA PLATAFORMA DE SUPERVISIÓN

CONFIGURACIÓN

El objetivo es limitar los elementos técnicos que pueden utilizarse para realizar un ataque, instalando únicamente los servicios y equipos indispensables.

Reforzar el nivel de seguridad requiere un endurecimiento que incluye:

- La limitación de las funciones de la plataforma
- El control de los elementos materiales de la plataforma

A. Modificación de la configuración predeterminada

Cada componente está configurado de acuerdo con los estándares, que incluyen:

- Cuentas técnicas y elementos de autenticación asociados
- Puertos de red utilizados
- Directorios de instalación y de trabajo
- Permisos de acceso a directorios y archivos.
- La cuenta utilizada para ejecutar un servicio o proceso, y los derechos asociados a esta cuenta
- Ficheros de configuración de elementos de seguridad, en particular, de trazabilidad.

B. Restricción de funciones accesibles

Solo los módulos indispensables para el funcionamiento y la seguridad de la plataforma se mantienen y están sujetos a una configuración adecuada, a un mantenimiento regular y a una supervisión.

El este sentido, el operador analiza el funcionamiento técnico de la plataforma para descartar los servicios o funciones que están instalados pero que no se usan.

Cada configuración de hardware o de software se inventaria en forma de configuración de referencia.

C. Inventario de elementos conectados

El operador realiza un inventario técnico completo de los elementos que constituyen la plataforma y los mapea. El inventario incluye los equipos que se pueden conectar a la plataforma de forma permanente o temporal, física o remota (puesto de trabajo, servidor, periférico, etc.).

En caso de que un tercero se conecte a la plataforma, el operador lo anota en su mapeo y lo tiene en cuenta en el análisis de riesgos.

D. Uso de elementos controlados

El operador gestiona los elementos directamente, incluyendo:
- El despliegue de actualizaciones
- La administración de elementos
- La configuración remota

DIVISIÓN

La plataforma sigue una lógica de segmentación al restringir cada subsistema a sus propias acciones para:
- Limitar la superficie de ataque
- Contener un posible ataque
- Limitar el impacto de un compromiso
- Permitir adaptar el nivel de seguridad de cada subsistema

La división se aplica tanto a medios físicos como lógicos.

A. Segmentación en subsistemas

La segmentación en subsistemas se realiza de acuerdo con los siguientes criterios:
- Funcionalidades
- Nivel de protección de datos
- Nivel de exposición
- Nivel de seguridad

Cualquier conexión entre subsistemas debe estar justificada por una necesidad funcional.

B. División física

Un servidor está dedicado a las aplicaciones más críticas

C. División lógica

Todos los datos almacenados en el servidor se cifran de antemano. Cada subsistema sigue su propio mecanismo de cifrado.

Toda la comunicación entre subsistemas pasa a través de la red privada virtual encriptada y autenticada.

ACCESO REMOTO

A. Acceso público

El acceso público sigue el protocolo HTTPS y la plataforma se autentica mediante la presentación de un certificado de servidor.

Para los usuarios de la plataforma se implementa la autenticación de doble factor.

B. Acceso móvil

Los puestos de trabajo móviles están configurados para establecer el túnel autenticado y encriptado hacia la plataforma. El túnel no se puede desactivar, y el acceso a Internet o a una red local es imposible.
La partición del sistema y la partición de los datos están totalmente cifradas.

La autenticación de doble factor está implantada en el puesto de trabajo.

FILTRADO DE RED

Además de la división, se implementan mecanismos de filtrado.

A. Puntos de filtrado

Las interconexiones entre subsistemas son los principales puntos de filtrado a los que se aplica el filtrado perimetral y local.

B. Reglas de filtrado

La matriz de flujo global incluye las reglas de filtrado vigentes. Esta se actualiza anualmente.

C. Implementación

El filtrado está garantizado por cortafuegos específicos basados en el principio de listas de autorización.