Panasonic
INDUSTRY

PANTALLAS TÁCTILES

Guía de ciberseguridad

Serie HM

Versión 1.0

Copyright y responsabilidad

Información de copyright y responsabilidad en relación con esta documentación.

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Alemania

Última modificación: 2024-07-23

Panasonic Industry Europe sigue una política de mejora continua del diseño y funcionalidad de sus productos. Por lo tanto, se reserva el derecho de modificar la documentación o el producto sin previo aviso. Panasonic Industry Europe no se hace responsable de posibles daños directos, especiales, incidentales o producidos como consecuencia de algún defecto del producto o de la documentación, incluso si se advierte de la posibilidad de dichos daños.

Para obtener asistencia técnica, contactar con Línea directa de Panasonic.

Tabla de contenidos

1 Acerca de este documento

A medida que aumenta la digitalización y la interconexión de redes, aparecen nuevos y más complejos riesgos internos y externos de ciberseguridad.

El BSI (German Federal Office for Information Security), por ejemplo, publicó un informe con las 10 principales amenazas, definiendo las reglas y recomendaciones para los equipos de red en los sistemas de control industrial (ICS):

- Infiltración de malware a través de dispositivos USB y hardware externo
- Infección por malware vía Internet e Intranet
- Fallos humanos y sabotajes
- Vulnerabilidad de seguridad de los componentes en la Extranet y en la nube
- Ingeniería social y phishing
- Ataques de Denegación de Servicio (DDoS)
- Componentes de control conectados a Internet
- Intrusión vía acceso remoto
- Fallos técnicos y de fuerza mayor
- Vulnerabilidad de seguridad de smartphones en entornos de producción

Fuente: https://www.bsi.bund.de/ICS

Este documento contiene la información del equipo necesaria para la gestión de la red y ayudará a proteger la pantalla táctil de la serie HM contra los riesgos de seguridad.

2 Política de seguridad de los productos Panasonic

Los productos y servicios de Panasonic siempre están en continua mejora. El desarrollo de nuestros productos sigue estrictamente las directivas de seguridad corporativas que incluyen un test exhaustivo antes del envío de los productos desde fábrica. La política de seguridad de Panasonic se basa en las guías internacionales recogidas en la IEC 62443 y ISO/IEC 27001.

El Panasonic Product Security Incident Response Team (Panasonic PSIRT) es el centro de coordinación de vulnerabilidades asociadas a los productos de Panasonic.

3 Configuración por defecto de la pantalla de la serie HM

La funcionalidad de red integrada en la pantalla táctil de la serie HM representa en sí misma un riesgo de seguridad. Para eliminar o minimizar este riesgo, se debe personalizar y reajustar la configuración de red por defecto.

- A partir de mayo de 2024 no se establecerá una contraseña por defecto, y la primera vez que se conecte al dispositivo tendrá que configurar una contraseña con un mínimo de reglas predefinidas. Las versiones anteriores cuentan con una contraseña predeterminada de fábrica, por lo que recomendamos cambiarla lo antes posible.
- Los puertos Ethernet están configurados como cliente DHCP.
- Por defecto, el módulo se suministra con los siguientes puertos abiertos y escuchando:

Nº de puerto	Protocolo	Función
80, 8000, 443	TCP/IP	Se utiliza en la página de configuración y en las páginas web de usuario
53	TCP/IP	Se utiliza para los servicios DNS
990-991	UDP	Se utiliza para el descubrimiento de dispositivos de red por difusión
21 (BSP 1.0 antes de 05/2024)	TCP/IP	Puertos de datos FTP (FTP modo pasivo: 16384-17407/TCP)
18756-18759	TCP/IP	Puertos de datos FTP protegidos
990 (a partir de BSP 1.3 05/2024)	TCP/IP	Tiempo de ejecución y gestión del proyecto

- Todas las funcionalidades y servicios, excepto la funcionalidad Scripts autoejecutables, de la pantalla táctil de la serie HM que podrían suponer un riesgo de vulnerabilidad, han sido deshabilitadas en fábrica. En IP/machine_config/#/services se puede ver un listado de los servicios.

Servicio	Riesgo de seguridad
Scripts autoejecutables	Programas que se ejecutan desde una unidad de almacenamiento externa p.ej. desde una memoria USB.
Demonio Avahi	Abre el puerto 5353 (se utiliza para recopilar información y encontrar características)
Servicios en la nube	P.ej., una configuración de un servidor OpenVPN utilizada con anterioridad
Servidor DHCP	Abre los puertos 67, 68
Servidor SNMP	Abre los puertos 161, 10161 (para la recopilación de información)
Servidor SSH	Abre el puerto 22 (Inicio de sesión con credenciales de administrador y ejecución de comandos)
Servidor VNC	Abre el puerto 5900 (Página web y control de dispositivos)

- Por defecto, el firewall implementado en la pantalla táctil de la serie HM (IP/machine_config/#/services) está deshabilitado.

- La pantalla táctil de la serie HM registra en los archivos de log, los datos e información relacionada con un funcionamiento atípico del dispositivo. Estos archivos se almacenan en el equipo y se pueden descargar accediendo con credenciales de administrador.

NOTA

Utilizar el firewall para cerrar los puertos no utilizados, y asegurarse de abrir e introducir el puerto Ethernet 443 en la configuración del firewall (para BSP 1.0, también se debe abrir el puerto 80). Si se cierran estos puertos, se denegará permanentemente el acceso a la página de configuración del sistema.

Temas relacionados

Configuración del Firewall (página 11)

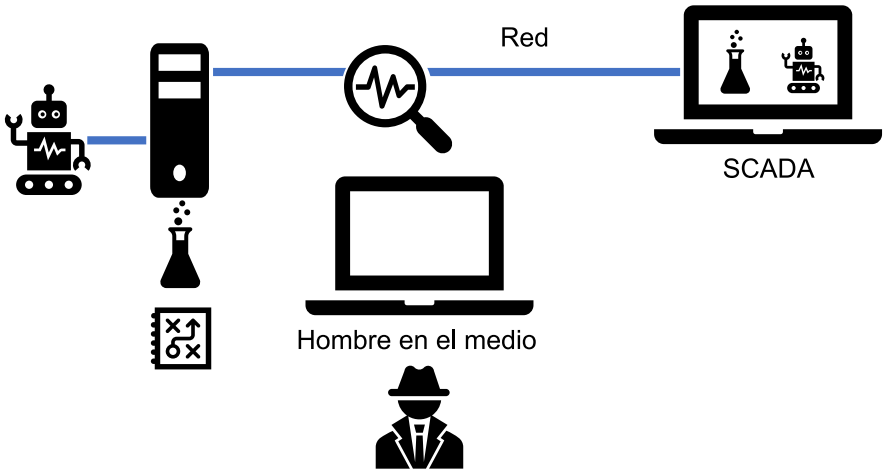
4 Escenarios de riesgos potenciales

Para una mejor comprensión y toma de conciencia de los riesgos potenciales de seguridad, a continuación se exponen algunos ejemplos típicos de ciberamenazas.

- Captura de datos

  Hoy en día existen multitud de herramientas para leer el tráfico de red, incluido el nombre de usuario, las contraseñas y otros datos sensibles como datos de proceso, recetas, etc.

  Especialmente si el tráfico de red no está encriptado, se convierte en un objetivo fácil para la captura de información disponible en la red por parte de espías.

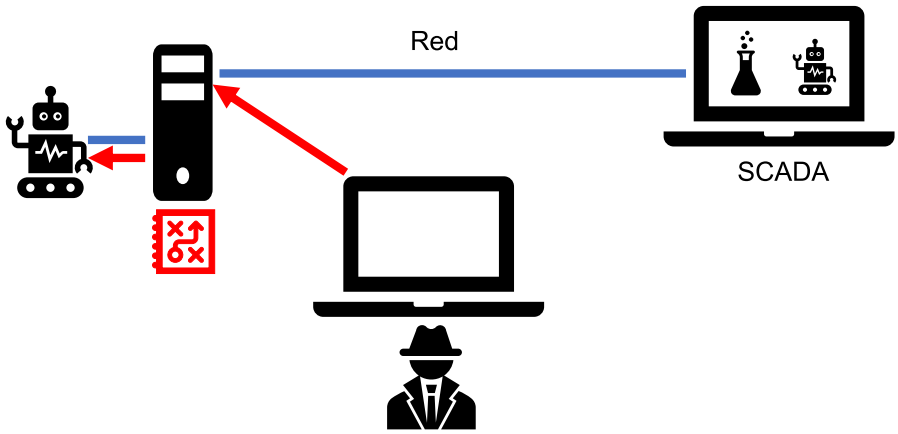


  Contramedidas:

  Nunca utilizar, para la transmisión de datos sensibles, protocolos FTP o Telnet fuera de una red encapsulada. Estos protocolos suponen un alto riesgo de seguridad ya que los nombres de usuario y las contraseñas se transmiten en texto plano.

- Acceso no autorizado a los sistemas de control

  Conociendo las credenciales o el protocolo utilizado, se pueden provocar fallos o sabotajes en las maquinas. Además, los dispositivos se pueden quedar secuestrados en una bonet (red de bots) para manipular o bloquear a otros dispositivos.

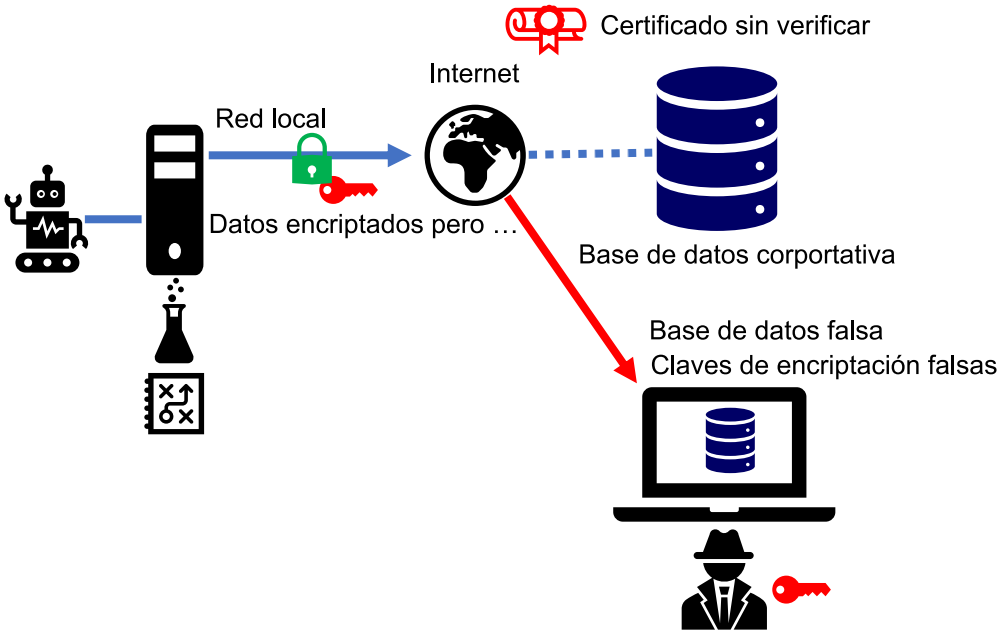


  Contramedidas:

  No permitir el acceso o el control desde equipos de terceros.

- Suplantación de identidad

  Las conexiones con páginas Web cuyas identidades no están verificadas por una autoridad de certificación pueden ser peligrosas puesto que son susceptibles de una suplantación de identidad y pueden redireccionar la comunicación. De esta forma, los atacantes pueden obtener información sensible (p. ej. usuarios, contraseñas, datos del proceso, o recetas). Con esa información se pueden causar daños graves manipulando las máquinas.



  Contramedidas:

  Siempre utilizar certificados para autenticar la identidad del servidor al que se pretende acceder.

5 Medidas de seguridad generales

La implementación de las medidas necesarias para proteger la red es crucial para el mantenimiento de la misma y para garantizar un tráfico seguro.

Puesto que este equipo se utiliza conectado a una red, se advierte de los siguientes riesgos de seguridad.

- Fuga o robo de datos a través del equipo.
- Uso de este equipo por personas malintencionadas para realizar operaciones ilegales.
- Interferencia o anulación de este equipo por parte de personas con intenciones maliciosas.
- Es responsabilidad del usuario tomar las precauciones necesarias como las descritas abajo para proteger la red de los riesgos de seguridad.
- Si se conecta este módulo a una red donde hay conectados ordenadores personales, asegurarse de que el sistema no se infecte por virus informáticos u otras entidades maliciosas (instalar un antivirus actualizado, programas antispyware, etc.).
- Utilizar este equipo en un entorno que tenga una LAN, una VPN (red privada virtual) o una red dedicada.
- Utilizar este equipo en un entorno al que solamente pueda acceder el personal con los privilegios de acceso legítimos.
- Utilizar este equipo y otros dispositivos conectados a través de la red como un PC, una tableta, etc. solamente si se han implementado las medidas de protección que garanticen la seguridad del sistema.
- No utilizar este equipo en lugares donde los cables o el propio equipo puedan ser dañados o inutilizados por personas con intenciones maliciosas.

Tener en cuenta que la configuración incorrecta de la conexión en la LAN existente, podría causar un funcionamiento incorrecto de los dispositivos de red. Consultar al administrador de la red antes de realizar la conexión.

En Internet hay información muy útil: MITRE ATT&CK® es una base de datos revisada y un modelo de comportamiento de los ciberadversarios.

6 Buenas prácticas para proteger la pantalla de la serie HM

Se pueden minimizar los riesgos de seguridad implementando las siguientes medidas preventivas y realizando la configuración adecuada del sistema y de las aplicaciones. Utilizar la lista de verificación que se proporciona en esta guía para garantizar que se toman todas las medidas necesarias para securizar la pantalla táctil de la serie HM.

Temas relacionados

Lista de verificación de la configuración de seguridad (página 14)

6.1 Ajustes del sistema

Ir a “System Settings” (Ajustes del sistema) (IP/machine_config) para configurar la contraseña y el firewall, para acceder a los archivos de log y para usar la funcionalidad de depuración SSH.

6.1.1 Protección por contraseña

Se debe modificar la contraseña por defecto por una contraseña robusta que incluya letras mayúsculas, minúsculas, números y caracteres especiales (excepto espacios en blanco).

Utilizar diferentes contraseñas de servidor FTP para las aplicaciones de HMWIN Studio y para los ajustes principales de la pantalla táctil de la serie HM. Cuando se enciende una pantalla por primera vez, se solicita la introducción de una nueva contraseña segura. Esto se puede hacer directamente en la pantalla o mediante un navegador conectado al equipo a través de su dirección IP (IP/machine_config).

6.1.2 Configuración del Firewall

Utilizar el firewall (IP/machine_config/#/services) para cerrar cualquier puerto que no se utilice.

Cuando se habilita el “Firewall Service” (Servicio Firewall) (IP/machine_config/#/services), se habilitan todas las funcionalidades vinculadas a las configuraciones y los puertos respectivos. Deshabilitar los servicios y puertos no utilizados o denegar el acceso a interfaces dedicadas (ETH0, ETH1, y ETH2).

NOTA

Comprobar que “Web Server – HTTP” y “Web Server – HTTPS” están habilitados y que el puerto Ethernet 443 está abierto (también el puerto 80 para BSP 1.0). Si se cierran estos puertos, se denegará permanentemente el acceso a la página de configuración del sistema.

Ejemplo de configuración del Firewall:

Nombre	Interfaz	Puerto o rango	Protocolo	Obligatorio
Servidor Web - HTTP (necesario para la configuración)	Cualquiera	80	TCP/IP	✓ (BSP 1.0)
Servidor Web - HTTPS (necesario para la configuración)	Cualquiera	443	TCP/IP	✓
Descubrimiento de dispositivos de red	Cualquiera	990–991	UDP	✓
Puerto comando FTP, necesario para operar con HMWIN Studio	Cualquiera	21	TCP/IP	✓ (BSP 1.0)
Modo FTP pasivo, necesario para operar con HMWIN Studio	Cualquiera	18756–18759	TCP/IP	
Servidor SSH	Cualquiera	22	TCP/IP	
Servidor VNC	Cualquiera	5900	TCP/IP	
Servidor DHCP	Cualquiera	67	UDP	
Servidor SNMP	Cualquiera	161	UDP	
Puertos de conexión del PLC	Cualquiera	9094–9097	TCP/IP	
Operaciones de HMWIN Studio	Cualquiera	990	TCP/IP	

6.1.3 Archivos de Log y funcionalidad de depuración SSH

Sirven para detectar operaciones atípicas. Solo se pueden utilizar con credenciales de administrador.

7 FAQ

1. ¿Se pueden obtener parches de seguridad y actualizaciones del firmware?

   Se pueden descargar las últimas actualizaciones desde la página web de Panasonic: Centro de descargas Panasonic o InfoHub

2. ¿El módulo dispone de algún tipo de puerta trasera?

   No. El módulo no tiene ninguna puerta trasera. Si se pierde la contraseña, no existe ninguna forma de recuperar la configuración.

3. ¿El módulo puede llamar a algún servidor de Panasonic?

   Con la configuración por defecto, no existe ningún proceso que llame automáticamente a un servidor de Panasonic.

4. ¿Dónde notificar una nueva vulnerabilidad?

   Contactar con el Panasonic Product Security Incident Response Team (Panasonic PSIRT), que es el centro de coordinación de vulnerabilidades asociadas a los productos de Panasonic.

8 Lista de verificación de la configuración de seguridad

Utilizar esta lista de verificación para garantizar que se toman todas las medidas necesarias para securizar la pantalla táctil de la serie HM. Marcar todos los elementos de la lista que estén implementados. Al final de la lista hay espacio para añadir elementos adicionales.

Hecho	Riesgo[1)]	Área	Página de configuración	Acción
	Alto	Contraseñas (administrador, usuario)	IP/machine_config/#/ authentication	Cambiar a contraseñas de administrador y usuario seguras
	Alto	Servicio: Scripts autoejecutables	IP/machine_config/#/services	Deshabilitar
	Alto	Servicio: Servidor SSH	IP/machine_config/#/services	Deshabilitar si no se necesita
	Bajo	Demonio Avahi	IP/machine_config/#/services	Deshabilitar si no se necesita
	Bajo	Servicios en la nube	IP/machine_config/#/services	Deshabilitar si no se necesita
	Bajo	Servidor DHCP	IP/machine_config/#/services	Deshabilitar si no se necesita
	Bajo	Servicio VNC	IP/machine_config/#/services	Deshabilitar si no se necesita
	Bajo	Firewall	IP/machine_config/#/services	Habilitar y personalizar la configuración
	Alto	Contraseñas HMWIN (al menos de administrador, usuario, log)	HMWIN Studio Project/Configuration/Security	Modificar las contraseñas de administrador y de usuario
	Alto	Configuración del protocolo	HMWIN Studio Project/Configuration/ Protocols	Desactivar las funciones de paso y los protocolos de servidor si no son necesarios. Seleccionar variantes encriptadas de los protocolos de bus de campo utilizados
	Medio	Funcionalidad HMWIN OPC UA	HMWIN Studio Project/Configuration/Interface	Comprobar el acceso al servidor
	Medio	Funcionalidad HMWIN MQTT	HMWIN Studio Project/Configuration/Interface	Utilizar encriptación y certificados

Hecho	Riesgo[1)]	Área	Página de configuración	Acción
	Medio	Funcionalidades SMTP y FTP Javascript	HMWIN Studio Comprobar los eventos configurados (p. ej., correo electrónico, FTP, cámara web...)	Utilizar encriptación y certificados

1) El riesgo depende de la aplicación.

9 Línea directa de Panasonic

Si tiene dudas o preguntas que no quedan suficientemente aclaradas en los manuales o en la ayuda online, póngase en contacto con una de nuestras oficinas de ventas.

Es de gran ayuda si junto con sus comentarios nos proporciona:

- El número de serie y/o el número de versión de su producto.
- Los números de paquete y versión de MS-Windows instalados en su ordenador.
- El tipo de hardware utilizado.
- El texto exacto de cualquier mensaje que aparece en la pantalla.
- Una descripción detallada del problema y de lo que ha hecho cuando este ha ocurrido.
- Qué pasos ha ejecutado para intentar resolver el problema.

Llame a la línea directa o utilice nuestro formulario de contacto para enviarnos su solicitud.

Para consultas fuera de Europa, visite nuestro sitio web global.

Panasonic Industry Europe GmbH

- Alemania y países europeos no incluidos en esta página:
  +49 89 45354-2748 (PLC, FP-I4C, pantallas táctiles)
  +49 89 45354-2737 (sensores)
  +49 89 45354-2750 (servoaccionamientos)
- Francia:
  +33 160 135757

Panasonic Industry Austria GmbH

Austria, Bosnia y Herzegovina, Bulgaria, Croacia, Eslovenia, Montenegro, Serbia y Suiza:

+43 2236 26846

Panasonic Industry Benelux B.V.

Bélgica, Dinamarca, Luxemburgo, Noruega, Suecia y Países Bajos:

+31 499 372727

Panasonic Industry Italia srl

Italia:

+39 045 6752711, support.piit@eu.panasonic.com

Panasonic Industry Poland sp. z o.o.

Países bálticos, República Checa, Finlandia, Hungría, Polonia, Rumanía y Eslovaquia:

+48 42 2309633

Panasonic Industry Iberia S.A.

Portugal, España:

+34 91 3293875

Panasonic Industry UK Ltd.

Reino Unido de Gran Bretaña e Irlanda:

+44 1908 231555

10 Histórico de cambios

Guía de ciberseguridad Versión 1.0, 2024.07	
	Primera edición