CECMED
CENTRO PARA EL CONTROL ESTATAL DE MEDICAMENTOS, EQUIPOS Y DISPOSITIVOS MÉDICOS
Ministerio de Salud Pública de Cuba

Departamento de Equipos y Dispositivos Médicos.
Sección de Vigilancia de Dispositivos Médicos

Comunicación del fabricante 017/2022

La Habana, 28 de junio de 2022
"Año 64 de la Revolución"

Ref: F202206016cu

Asunto: Comunicación del fabricante según notificación de calidad QN-RDS-POC-2022-063
Producto afectado: cobas b 221<2>=Roche OMNI S2 system
cobas b 221<4>=Roche OMNI S4 system
cobas b 221<6>=Roche OMNI S6 system
Número de lote: NP
Fabricante: Roche.
Titular: Roche.

Descripción:

El fabricante Roche, a través de su representación en Cuba ha enviado la notificación de calidad QN-RDS-POC-2022-063 referida a posibles riesgos para la privacidad de datos en el ámbito del cobas b 221, versiones del software ≤8.04 y versión del software futura 8.05.
Durante el desarrollo de parche de servicio de la versión del SW 8.05 del cobas b221, se realizaron pruebas de penetración según lo establecido en el proceso actual para la liberación de una versión del SW nueva. Estas pruebas revelaron posibles vulnerabilidades en el cobas b221, versiones del software ≤8.04 y versión del software futura 8.05.
El impacto de estas vulnerabilidades puede dar lugar a un riesgo de acceso no autorizado a datos de los pacientes y credenciales de los operadores. Existe un riesgo teórico de manipulación de datos de los pacientes.
Roche ha estado realizando investigaciones de estas vulnerabilidades y evaluando los riesgos asociados a ellas y recomienda implementar contramedidas específicas para mitigar el riesgo. La ciberseguridad de los dispositivos médicos es una responsabilidad compartida entre varias partes interesadas, incluidos los centros sanitarios, los proveedores y los fabricantes de dispositivos médicos.

Acciones requeridas para solucionar el problema:

Roche ha emitido la comunicación correspondiente para sus clientes con el objetivo de mitigar, con su ayuda, los riesgos de ciberseguridad.
Los clientes deben restringir el acceso físico al sistema y a todas las infraestructuras informáticas vinculadas. Además, para evitar todo riesgo de intrusión en el sistema por un atacante que hubiera obtenido las credenciales de un operador, los clientes deben configurar cortafuegos para bloquear todo tráfico de la red hasta el sistema cobas b 221 system que no proceda de servidores autenticados (p. ej., POC IT, LIS systems). Debe asegurarse que las redes vinculadas son seguras y tenerse en cuenta las directrices locales sobre una contraseña segura.

Calle 5ta A, Número 6020, entre 60 y 62, Reparto Miramar, Municipio Playa, La Habana. CP 11300
Telef: (537) 2164100 E-mail: cecmed@cecmed.cu Web: www.cecmed.cu

Los operadores, que tienen acceso al sistema, deben recibir formación según se indica en la sección de información de seguridad de las instrucciones de uso. Los clientes son responsables de la seguridad informática de su infraestructura informática y de protegerla frente al ataque por softwares malintencionados y piratas informáticos.
Reportar incidentes relacionados con su representante local de Roche.
Los clientes tienen que ser informados sobre este problema. No se requieren comentarios para esta Notificación de Calidad.
En cualquier caso de quejas por parte de los clientes, debe escalarse como incidencia global.

Acciones para garantizar que los usuarios dispongan de la información:

La empresa garantizará la notificación de esta situación a todos los clientes de la Red Nacional de Salud a través de la Comunicación del Fabricante.
El CECMED mediante el Sistema de Vigilancia Postcomercialización, emite el presente documento para su divulgación a todo el Sistema Nacional de Salud, al que se adjunta la comunicación original de Roche.
Los usuarios que identifiquen el producto entre su stock de dispositivos, deben notificar vía correo electrónico al CECMED, que han recibido la comunicación y han implementado las medidas recomendadas por el fabricante, así como otras necesarias para su divulgación al personal que emplea el producto.

El envío de notificaciones relacionadas con este u otros dispositivos médicos, se hará a la Sección de Vigilancia de Dispositivos Médicos del CECMED mediante correo electrónico dirigido a la dirección: **centinelaeq@cecmed.cu** o mediante los teléfonos **72164364 / 72164365**.
En el caso de diagnosticadores el que reporta lo hará mediante el llenado del Formulario REM-IVD.

Distribución: Director Nacional de Medicamentos y Tecnologías Médicas, Director Nacional de Atención Médica, Jefe del Departamento Nacional de Hospitales, Centro Nacional de Electromedicina, Grupo Nacional de Laboratorio Clínico, Personal especializado y Coordinadores de los Comité de Seguridad de Equipos Médicos a nivel institucional.

Aprobado por:

Dr. Mario Cesar Muñiz Ferrer
Jefe de Departamento de Equipos y Dispositivos Médicos
CECMED

Calle 5ta A, Número 6020, entre 60 y 62, Reparto Miramar, Municipio Playa, La Habana. CP 11300
Telef: (537) 2164100 E-mail: cecmed@cecmed.cu Web: www.cecmed.cu

Aviso al cliente

Ref No:	**QN-RDS-POC-2022-063**
Versión	**1**
Fecha del documento:	**30-may-2022/Aplicaciones**

PRODUCTO AFECTADO:

cobas b 221<2>=Roche OMNI S2 system
cobas b 221<4>=Roche OMNI S4 system
cobas b 221<6>=Roche OMNI S6 system

RESUMEN DEL PROBLEMA:

Esta Notificación de Calidad incluye información sobre posibles riesgos para la privacidad de datos en el ámbito del cobas b 221, versiones del software ≤8.04 y versión del software futura 8.05.
El impacto de estas vulnerabilidades puede dar lugar a un riesgo de acceso no autorizado a datos de los pacientes y credenciales de los operadores. Existe un riesgo teórico de manipulación de datos de los pacientes.

ACCIONES REQUERIDAS:

Información al cliente. Reportar incidentes relacionados con su representante local de Roche o al CEAC.
Los clientes tienen que ser informados sobre este problema. No se requieren comentarios para esta Notificación de Calidad.
En cualquier caso de quejas por parte de los clientes, debe escalarse como incidencia global.

CONTACTOS:

Centro de Excelencia en Atención al Cliente CEAC: 50815864 y 01800-7188853 ó 54
HOSPOC – Hub México

Apreciado cliente:

Reciba cordial saludo de nuestra parte.

Tenemos información importante que queremos compartir con usted.

Durante el desarrollo de parche de servicio de la versión del SW 8.05 del cobas b 221, se realizaron pruebas de penetración según lo establecido en el proceso actual para la liberación de una versión del SW nueva. Estas pruebas revelaron posibles vulnerabilidades en el cobas b 221, versiones del software ≤8.04 y versión del software futura 8.05.

Roche ha estado realizando investigaciones de estas vulnerabilidades y evaluando los riesgos asociados a ellas y recomienda implementar contramedidas específicas para mitigar el riesgo. La ciberseguridad de los dispositivos médicos es una responsabilidad compartida entre varias partes interesadas, incluidos los centros sanitarios, los proveedores y los fabricantes de dispositivos médicos. En consecuencia, por la presente Roche se comunica con los clientes para mitigar con su ayuda estos riesgos de ciberseguridad.

Los clientes deberían restringir el acceso físico al sistema y a todas la infraestructuras informáticas vinculadas. Asimismo, para evitar todo riesgo de intrusión en el sistema por un atacante que hubiera obtenidos las credenciales de un operador, los clientes deberían recibir instrucciones para configurar su cortafuegos para bloquear todo tráfico de la red hasta el sistema cobas b 221 system que no proceda de servidores autenticados (p. ej., POC IT, LIS systems). Debe asegurarse que las redes vinculadas son seguras y tenerse en cuenta las directrices locales sobre una contraseña segura. Los operadores, que tienen acceso al sistema, deben recibir formación según se indica en la sección de información de seguridad de las instrucciones de uso. Véanse las páginas 29-31 de las instrucciones de uso (versión 19 para el resto del mundo, versión 5 para EE. UU.). Los clientes son responsables de la seguridad informática de su infraestructura informática y de protegerla frente al ataque por softwares malintencionados y piratas informáticos.

Esperamos que la información proporcionada sea útil. Le pedimos disculpas por cualquier inconveniente causado por este problema. Agradecemos su comprensión y apoyo.

Atentamente,

Antonio Moreno
Hospoc Sr. Application Specialist
CEAC

_____

Nombre y fecha de recibo

_____

Firma