BOLETÍN DE ALERTAS DE CIBERSEGURIDAD Y SALUD.

#41 BOLETÍN
ENERO 2023

Bienvenido al boletín de alertas de ciberseguridad y salud de S2 Grupo.
El objetivo es que os resulte de utilidad y que, entre todos, podamos aportar contenidos interesantes específicos para el sector de la salud. Este boletín nace como canal de comunicación con nuestros clientes y por eso preferimos, de momento, que sea a través del correo electrónico, pero siéntete libre de compartirlo con otros colegas a los que pienses que les puede ser de interés: **La seguridad sigue siendo cosa de todos.**

"En este arranque del año ya hemos vivido grandes incidentes de ciberseguridad dentro del sector salud, ataques a hospitales, brechas de datos e importantes advertencias acerca de grupos de ciberdelincuencia. 2023 ha llegado plagado de retos, pero ello nos recuerda la importancia de trabajar juntos."

NOTICIAS

1. El grupo creador del ransomware LockBit se disculpa y ofrece la clave de cifrado de manera gratuita al hospital de niños más grande de Canadá tras verse afectado por su ransomware. Un partner de este grupo de ransomware-as-a-service, uniéndose al programa de afiliados de LockBit, lo utilizó para un ataque definido como poco ético por los desarrolladores. Inglés1 / Inglés2.

2. El hospital Howard Memorial de Nashville, Arkansas, detectó una actividad sospechosa en su red. La información de pacientes y empleados podría haber sido comprometida. Los archivos contenían nombres de pacientes, información de contacto, números de la seguridad social, información del seguro, historial médico, etc. Inglés1 / Inglés2

3. También en Colombia, la compañía farmacéutica Audifarma encargada de entregar medicamentos a 12 millones de pacientes fue objeto de un ciberataque. El ataque ha afectado a la comunicación para la entrega de medicamentos a los usuarios. Sin embargo, Audifarma afirma que los datos de los pacientes no fueron comprometidos. Español1 / Español2

4. BlackCat, el grupo de ransomware que combina ataques de ransomware con amenazas de filtración de datos e inutilización de sitios web, atacó al proveedor de HCE NextGen Healthcare. NextGen dijo que el grupo de ransomware no obtuvo datos de ningún cliente. Sin embargo, BlackCat puso una muestra de información de NextGen en su sitio de extorsión.

   Por otro lado, el Centro de Coordinación de Ciberseguridad del Sector Sanitario emitió un informe el 12 de enero en el que advertía al sector sanitario sobre las tácticas y técnicas de explotación utilizadas por los programas Royal y BlackCat, dos grupos de ransomware que han estado atacando agresivamente al sector sanitario estadounidense. Inglés1 / Inglés2 / Inglés3

ALERTAS

VENDEDOR	SISTEMA	CRITICIDAD	DESCRIPCIÓN	FUENTE
Philips	Centro de Información de Philips iX (PIC iX) y monitores de la serie Efficia CM	MEDIA	La explotación con éxito de estas vulnerabilidades puede permitir a un atacante el acceso no autorizado a los datos (incluidos los datos del paciente) y crear una denegación de servicio que resulte en la interrupción temporal de la visualización de los datos fisiológicos en la estación central. La explotación no permite modificar ni cambiar los dispositivos de los puntos de atención.	Inglés

BOLETINES Y ACTUALIZACIONES

VENDEDOR	PUBLICACIÓN	DETALLES
Oracle		Boletín
Microsoft		Actualizaciones

PENSAMOS QUE PODRÍA INTERESARTE

1. Durante el 2022, los proveedores tecnológicos del sector sanitario han jugado un papel protagonista en la ciberseguridad de estas infraestructuras y algunas estadísticas reflejan que el 55% de las organizaciones sanitarias ha sufrido brechas debido a ellos. Fugas de datos, brechas en la nube y ataques IoT son las tres vulnerabilidades principales en este sector. Inglés.

2. Desde S2 Grupo lanzamos nuestro Cyber Threat Intelligence Report - Tendencias Q4 2022, donde se recoge la actividad más significativa detectada en el último trimestre del año por los especialistas de Lab52, nuestra división de Threat Intelligence. Español /Inglés.

¿Echas de menos alguna información que te gustaría que incluyéramos?
¿Quieres que entrevistemos a alguien de referencia en el mundo de ciberseguridad y salud?
¿Quieres compartir alguna iniciativa interesante de tu organización?

Escríbenos a **clientes@s2grupo.es** y haznos llegar tu propuesta.

S2 GRUPO
Anticipando un mundo **ciberseguro**