CERT ONESEQ RFC 2350

Este documento contiene una descripción del Centro de Respuesta a Incidentes de OneseQ, en adelante OneseQ_CERT, según el RFC 2350.

A su vez, proporciona información básica sobre el OneseQ_CERT las formas en las que se puede contactar con él, su comunidad objetivo y los servicios ofrecidos.

1. Información del documento

1.1. Fecha de la última actualización

Esta es la última versión 1.0 del 10 de enero de 2020.

1.2. Listas de distribución

No existe ninguna lista de distribución para notificar cambios en el documento. Los cambios son anunciados en https://oneseq.es .

1.3. Ubicación del documento

La última versión de documento se encuentra publicada en:

- Español:
https://www.oneseq.es/wp-content/uploads/2022/04/CERT_OneseQ_RFC_2350_ES.pdf

- Inglés:
https://www.oneseq.es/wp-content/uploads/2022/04/CERT_OneseQ_RFC_2350_EN.pdf

2. Información de Contacto

2.1. Nombre del Equipo

OneseQ_CERT

2.2. Dirección

Calle Albasanz 16 planta 4, 28037 Madrid, España

2.3. Zona horaria

CET / CEST

2.4. Número de teléfono

+34 917 872 300

2.5. Direcciones de Correo Electrónico

Intercambio de información relativa a incidentes: soc@oneseQ.es

Consultas de carácter general: soc@oneseQ.es

Otras direcciones de correo electrónico para contactar se encuentren publicadas en https://oneseq.es/contacto

2.6. Claves Públicas y cifrado de la información

Se encuentran publicadas en https://oneseq.es

2.7. Miembros del equipo

Los nombres e información de los miembros que componen el OneseQ_CERT no son difundidos públicamente. En el caso de que se realice algún reporte, el personal se identificará con su nombre completo a través de una comunicación formal

2.8. Puntos de contacto para la comunidad

El método de contacto preferido para la comunicación con el CERT de OneseQ es el correo electrónico.

Por favor, escríbanos a la cuenta soc@oneseq.es con la llave pública. Esto nos permite crear un caso en nuestro sistema de ticketing y que sea tratado por nuestro personal.

3. Constitución

3.1. Misión

Ofrecemos servicios de ciberseguridad para infraestructuras críticas, instituciones educativas, instituciones públicas y corporaciones privadas, además ofrecemos servicios de seguridad de la información, analizamos eventos e incidentes de seguridad, coordinamos soluciones técnicas, aseguramos perimetralmente las infraestructuras OT y IT de nuestros clientes y adiestramos a otros equipos en la gestión de equipos de seguridad.

3.2. Comunidad a la que brinda servicios

Nuestros servicios de Ciberseguridad se prestan a clientes finales, tanto a empresas privadas (industria, infraestructuras críticas, integradores con proveedores de soluciones de

ciberseguridad e integradores con proveedores de telecomunicaciones) y organismos públicos (ayuntamientos, hospitales…).

3.3. Patrocinio / Afiliación

El CERT/SOC de OneseQ es un área de la Empresa Alhambra IT y es el encargado de dar respuestas a incidentes.

3.4. Autoridad

Cada miembro del equipo tendrá su propio código identificador asignado para cada poder identificar cada trabajo realizado.

El equipo cuenta con personal N1, N2 Y N3.

Los N1 son los encargados de la gestión del día a día, monitorizan las unidades de información en busca de anomalías, reciben y gestionan las alertas.

Los N2 son los encargados de emitir los informes en base a los resultados temporales obtenidos por las monitorizaciones. Fuera de su horario son los encargados de las guardias, responder a las solicitudes telefónicas de los clientes, cada uno de los cuales tiene su propio PIN de comunicación.

Los N3 son especialistas, analizan las alertas y los incidentes registrados. Se encargan de coordinar a los N1 y los N2.

Cada operador tendrá asignadas unas tareas dentro del CSIRT, para las que estarán perfectamente preparados para gestionar la tarea desde el inicio, las tareas las repartirá y serán seguidas por el responsable.

4. Políticas

4.1. Tipo de incidentes y nivel de soporte

El CERT de OneseQ, evalúa los incidentes mediante avisos y alertas de seguridad recogidas por nuestro servicio SOC, lo que nos permite involucrarnos en la coordinación y respuesta entre el OneseQ CERT para dar una respuesta/solución a dichos incidentes.

4.2. Cooperación, Interacción y divulgación de la Información

La información es tratada con absoluta confidencialidad, siempre dentro de las políticas y procedimientos establecidos y predefinidos. Siempre con la cooperación entre distintos equipos CSIRT.

4.3. Comunicación y Autenticación

Los medios disponibles para la comunicación con OneseQ_CERT son el correo electrónico cifrado con la clave pública dedicadas para ello y publicadas en el portal https://oneseQ.es y correo electrónico a la dirección: soc@oneseQ.es

5. Servicios

Ver documento:

https://www.oneseq.es/wp-content/uploads/2022/04/CSIRT_OneseQ_descripcion_del_servicio.pdf

5.1. Respuesta al Incidente

5.1.1. Noticias

Desde OneseQ_CERT se promueve la divulgación de información en temas relacionados con la aparición de nuevas vulnerabilidades publicadas, vectores de ataque, nuevas herramientas de seguridad…Todo ello pensado para proteger sistemas informáticos y de redes y/o relacionados con seguridad de la información.

5.2. Alertas y/o advertencias

OneseQ_CERT proporciona y difunde información sobre ciberseguridad, vulnerabilidades y se proporciona soluciones de consultoría para abordar problemas con servicios de seguridad.

6. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- Buzón de correo específico: soc@oneseQ.es
- Teléfonos proporcionados mediante el proceso de contratación o adhesión al CERT de OneseQ.

7. Descargo de Responsabilidades

El Equipo OneseQ CERT no se responsabiliza del mal uso que pueda darse de la información aquí contenida.