CERT ONESEQ RFC 2350

This docment contains a description of the OneseQ Incident Response Center, hereinafter OneseQ_CERT, according to RFC2350.

At the same time, it provides basic information about the OneseQ_CERT, the ways in which it can be contacted, its target community and the services offered.

1. Document Information

1.1. Date of last update

This is the latest versión 1.0 on January 10, 2020.

1.2. Distribution lists

There is no distribution list to notify changes to the document. Changes are announced at https://oneseq.es

1.3. Document location

The latest versión of the document is published at:

- Spanish version: https://www.oneseq.es/wp-content/uploads/2022/04/CERT_OneseQ_RFC_2350_ES.pdf
- English version: https://www.oneseq.es/wp-content/uploads/2022/04/CERT_OneseQ_RFC_2350_EN.pdf

2. Contact

2.1. Team's name

OneseQ_CERT

2.2. Address

Calle Albasanz 16 planta 4, 28037 Madrid, Spain

2.3. Time Zone

CET / CEST

2.4. Phone Number

+34 917 872 300

2.5. Email addresses

- Exchange of incident information: soc@oneseQ.es

- General inquiries: soc@oneseQ.es
- Other email addresses: https://oneseQ.es/contacto

2.6. Public keys and information encryption

Keys are published https://oneseq.es

2.7. Team members

The names and information of the members that make up the OneseQ_CERT are not publicly disseminated. In the event that a report is made, the staff will be identified with their full name through a formal communication.

2.8. Contact point for community

The preferred contact method for comunication with the OneseQ CERT is email.

Please write to us at the account soc@oneseq.es whit the public key. This allow us to create a case in our ticketing system and have it handled by our staff.

3. Constitution

3.1. Mission

We offer cybersecurity services for critical infrastructures, educational instituions, pubilc institutions and private corporations, we also offer information security services, analyze security events and incidents, coordinate technical solutions, secure the perimeter of our clients'OT and IT infraestructures and train others in the mangement of security equipment.

3.2. Community served

Our Cybersecurity services are provided to end customers, both to private companies (industry, critical infrastructures, integrators with cybersecurity solution providers and integrators with telecommunications providers) and public bodies (city councils, hospitals...).

3.3. Sponsorship/Affilation

The OneseQ CERT/SOC is an area of the Alhambra IT Company and is in charge of responding to incidents.

3.4. Autorithy

Each member of the team will have their own assigned identification code to be able to identify each work carried out.

The team has N1, N2 and N3 personnel.

The N1s are in charge of day-to-day management, monitoring the information units in search of anomalies, receiving and managing alerts.

The N2 are in charge of issuing the reports based on the temporary results obtained by the monitoring. Outside their hours they are in charge of the guards, responding to telephone requests from customers, each of whom has their own communication PIN.

The N3 are specialists, they analyze the alerts and the recorded incidents. They are in charge of coordinating the N1 and the N2.

Each operator will be assigned some tasks within the CSIRT, for which they will be perfectly prepared to manage the task from the beginning, the tasks will be distributed and will be followed by the person in charge.

4. Policies

4.1. Types of incidents and Support level

The OneseQ CERT evaluates the incidents through security warnings and alerts collected by our SOC service, which allows us to get involved in the coordination and response between the OneseQ_cert to provide a response/solution to said incidents.

4.2. Cooperation, Interation and disclosure of information

The information is treated with absolute confidentiality, always within the established and predefined policies and procedures. Always with the cooperation between different CSIRT teams.

4.3. Communication and Authentication

Any incident, alert or notice must be sent with the public key, which is shared in the web site https://oneseq.es and using this specific email address: soc@oneseq.es

5. Servicies

See the next document:

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

5.1. Incident response

5.1.1. News

OneseQ_CERT promotes the disclosure of information on issues related to the appearance of new published vulnerabilities, attack vectors, new security tools... All of this designed to protect computer systems and networks and/or related to information security.

5.2. Alerts and/or warnings

OneseQ_CERT provides and disseminates information on cybersecurity, vulnerabilities and consulting solutions are provided to address problems with security services.

6. Incident reporting form

Incident reporting can be done by:

- Specific email address: soc@oneseQ.es
- Phone numbers provided through the OneseQ CERT contracting or joining process.

7. Disclaimer

The OneseQ CERT Team is not responsible for the misuse that may occur of the information contained herein.