CSIRT DESCRIPTION FOR NAVAL GROUP CERT

RFC 2350 V1.0

NAVAL GROUP

Summary

1. Document information

This document contains a description of Naval Group CERT according to RFC 2350. It provides information about the CSIRT, how to contact the team, and describes its responsibilities and services offered by Naval Group CERT.

1.1 Date of the Last Update

This is the version 1.0 released on July, 08th 2019

1.2 Distribution List for Notifications

Notification of document changes is not distributed by a Mailing List or any other mechanisms.

1.3 Location where this Document May be Found

The current document version of this document is available on Naval Group Website:

https://www.naval-group.com/fr/innovation/nos-equipes/computer-security-information-response-team/

1.4 Document authenticity

This document is signed with the Naval Group CERT PGP Key.

2. Contact information

2.1 Name of the team

The registered name of the team is **Naval Group CERT** and the short name is "**NavCERT**".

2.2 Postal Address

Naval Group CERT

Direction Cybersécurité

199 avenue Pierre Gilles de Gennes

83190, Ollioules, France

2.3 Date of Establishment

Naval Group CERT was established on September 2017

2.4 Time Zone

CET/CEST: Europe/Paris(GMT+01:00, and GMT+02:00 on DST)

2.5 Telephone Number

+33 494 116 622

2.6 Facsmile Number

None available

2.7 Other Telecommunication

None available

2.8 Electronic Mail Address

cert@naval-group.com

2.9 Public Keys and Encryption Information

Our current PGP-Key is available under request by sending an email at cert@naval-group.com or could be retrieved from one of the usual public key server such as http://pgp.mit.edu/

Key ID: 0x3167396E

Fingerprint: 5DA5549E895551A9FD21E478F3ADC40131673FB5

2.10 Team Members

The Naval Group CERT Representative is Pascal Mercier. and CERT Coordinator is Julien Vignolles.

The full list of the team members is not publicly available. The team is made of Cybersecurity analysts.

2.11 Other information

None

2.12 Points of Customer Contact

Naval Group CERT is able to receive incident or vulnerability reports via e-mail. Please use our cryptographic key to ensure authenticity and confidentiality.

Naval Group CERT operates during regular business hours (9:00 AM-6:00 PM GMT+1 from Monday to Friday).

3. Charter

3.1 Mission Statement

The Naval Group CERT Team's activities are non-profit and fully financed by Naval Group S.A.

The mandate of Naval Group CERT is to:

- Control cybersecurity risks by providing active cyber threat intelligence and cybersecurity survey activities for the whole Naval Group and subsidiaries
- Prevent and anticipate cyber security incident by providing a strong expertise on technical security audit and vulnerability hunting.
- Investigate, respond and coordinate cybersecurity incident which can affect Naval Group's asset, customers, employees and shareholders, according the laws and regulations that may apply.

3.2 Constituency

Our constituency is composed of Naval Group and all its subsidiaries.

3.3 Sponsorship or Affiliation

Naval Group CERT is a private CERT in the naval sector. It is owned, operated and financed by Naval Group S.A

It maintains relationships with different CSIRTs in France and in Europe.

3.4 Authority

Naval Group CERT operates under the auspices, and with the authority delegated by the Cybersecurity CTO. Naval Group CERT is responsible for coordinating the incident response, threat prevention and proactive audit across the company for all perimeters.

4. Policies

4.1 Type of Incidents and Level of Support

Naval Group manages all type of cybersecurity incidents which occur, or theaten to occur, within its constituencies.

The level of support depends on the type and severity of the given security incident, the amount of affected entities, and our resources at the time.

Usually our acknowledgement is delivered on the same working day, or the day after, during working hours.

4.2 Co-operation, Interaction and Disclosure of Information

Naval Group CERT exchanges all necessary non-restricted information with other CSIRTs as well as with other affected parties involved on in the incident or incident response process.

No incident or vulnerability related information will not be publicly disclosed without the agreement of all involved parties.

Legal requests will be assessed by our legal council and an appropriate response will be given if the request is acceptable, within the limits of the court order, the related criminal investigation and the requested information.

4.3 Communication and Authentication

Naval Group CERT strongly encourage you to send email signed using PGP-Key.

All email-s containing restricted information must be encrypted using PGP-Key.

For general non-restricted communication, a phone-call, postal service, or unencrypted email may be used.

Naval Group CERT supports the Information Sharing Traffic Light Protocol (TLP).

5. Services

5.1 Incident Response

The team offers the following services:

- Incident handling
- Incident analysis (including technical forensics and malware analysis)
- Incident response coordination
- Vulnerability response coordination

5.2 Proactive Defense

- Penetration testing
- Artefact handling and analysis
- Threat hunting

5.3 Alerts, Warning and Cyber Threat Intelligence

- Building, sharing IOCs and signatures
- Knowledge gathering on cyber threat actors
- Dissemination of cyber threats information
- Awareness building
- Cyber security alerts publication

6. Incident Reporting Forms

Naval Group CERT does not have public incident reporting form. We encourage you to report any security incidents via encrypted e-mail to cert@naval-group.com

Incident reports must contain the following information:

- Incident date and time (including time zone)
- Description of the incident

- Source/Destination IPs, ports and protocols or the affected product
- Any relevant information.

7. Disclaimers

This document is provide ‘as is’ without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

If you notice any mistakes within this document please send a message to us by e-mail. We will try to resolve such issues as soon as possible.