GRIMALDI GROUP S.p.A.

RFC 2350 G-SIRT

EXPECTATION FOR COMPUTER SECURITY INCIDENT RESPONSE

TITLE: RFC 2350 G-SIRT
DATE: 10/07/2019
VERSION: 2.0

Expectation For Computer Security Incident Response

1 - DOCUMENT INFORMATION

1.1 Version

Version is 2.0

1.2 Distribution List

Notification of updates are submitted to the mailing list: soc[at]enav.it, cert[at]garr.it, soc[at]gse.it, ti[at]rusted-introducer.org .

1.3 Location where this document may be found

A copy of this document could be requested sending an email to csirt[at]grimaldi.napoli.it.

The current version of this document can be found at https://www.grimaldi.napoli.it/download/G-SIRT RFC2350.zip

1.4 Authenticating this Document

This document has been signed with PGP key of G-SIRT. See section 2.8 for more details.

1.5 Document Identification

Title: "RFC 2350 G-SIRT"

Version: 2.0

Document Date: November 2019

Expiration: This document is valid until superseded by a later version

2 - CONTACT INFORMATION

2.1 Name of the team

Grimaldi Security Incident Response Team

Short name: G-SIRT

2.2 Address

Postal Address

G-SIRT at Grimaldi EUROMED

Grimaldi EUROMED

Via Marchese Campodisola, 13

80133 - Napoli

Italy

2.3 Timezone

Central Europe Time/Central Europe Summer Time

2.4 Telephone number

+39 081 496787

2.5 Fax number

Fax number is provided for a restricted group of contacts.

2.6 Electronic email address

G-SIRT can be reached via csirt[at]grimaldi.napoli.it

All messages sent to this email address are received by all G-SIRT members.

2.7 Other telecommunications

None.

2.8 Public Keys and encryption information

PGP key is used for functional exchanges between G-SIRT and other parties:

ID: 0x856976AD

Fingerprint: EC7D 2F4E 381F DB0C E7AC 729E 908A 4F31 7314 FFB8

2.9 Team members

G-SIRT is an Incident Response Team for the private sector Transportation & Logistic. It is operated by Grimaldi EUROMED,a Grimaldi Group company. The team is made up of Cyber Security Analysts, Security Engineers and Incident Responders.

2.10 Other information

None.

2.11 Point of Customer Contact

The preferred method for contacting G-SIRT is via email at csirt[at]grimaldi.napoli.it . The mailbox is monitored during regular office hours: Monday to Friday. 08:30-17:30, except during public holiday in Italy. If you required urgent assistance, put "urgent" in your subject line or contact by telephone during regular office hours. Please, use PGP/GPG if you need to send sensitive information.

3 - CHARTER

3.1 Mission statement

G-SIRT's mission is to defend its constituency against cyber threat. It suggests and implements security tactical and technical countermeasures in order to prevent and protect any violation attempt having an impact for Grimaldi information asset.

G-SIRT main targets are:

- Effective responsiveness in case of incidents and maximum commitment to resolve the issues.
- Provide information on potential threat impacting the information assets of Grimaldi Group.
- Facilitating the exchange of good practices between constituents and with peers.
- Increase the awareness and security culture for Grimaldi Group.

3.2 Constituency

G-SIRT constituency refers to the users, systems and applications and any other relevant resources of Grimaldi Group and the companies belonging to the same group. Vessels owned by "Grimaldi Euromed" and "Grimaldi Deep Sea" are included into constituency only.

3.3 Sponsorship and/or affiliation

G-SIRT is managed by Security Team under control of Grimaldi EUROMED IT Department.

3.4 Authority

G-SIRT achieves its functions through the services delivered to its constituency, the collaboration with authoritative CERTs, peers, Information Security community, Law Enforcement and Service Providers.

G-SIRT is authoritative for "Grimaldi EUROMED" and "Grimaldi Deep Sea", meanwhile it acts as an advisory for all the other companies owned by Grimaldi Group, especially: "Atlantic Container Line", "Malta Motorways of the Sea", "Minoan Lines" and "Finnlines".

4 - POLICIES

4.1 Types of Incidents and Level of Support

G-SIRT is authorized to address all types of information security incidents that occur within its constituency, according to agreements and mandates defined with constituency members. G-SIRT is also committed to keeping its constituency informed of relevant vulnerabilities, emerging threats and trends, and where possible, it will inform them of such criticalities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

G-SIRT receives incident reports related to events or threats impacting Grimaldi Group, then it classifies and evaluates incident severity, and in accordance to triage, informs the appropriate management level. It also coordinates the activities needed to put in place appropriate incident resolution. G-SIRT takes into account with regards to the handling and disclosure of information applicable laws of Italy, in order to not cause any injury.

G-SIRT shall exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. Neither personal nor further data are exchanged unless explicitly authorized.

4.3 Communication and Authentication

G-SIRT protects sensitive information in accordance with relevant regulations and policy within the EU. Conventional method such as unencrypted emails are suitable for exchange of low sensitive information.

To exchange high-sensitivity information an encrypted email with PGP/GPG keys is mandatory required.

G-SIRT recognize and support the ISTLP (Information Sharing Traffic Light Protocol). It will treat all submitted information as TLP:AMBER per default, and will only forward it to concerned constituency members or parties in order to resolve specific incidents when an acknowledge is implicit or expressly given.

5 - SERVICES

5.1 Incident Response

G-SIRT provide assistance and support to manage cyber security incidents impacting its constituency, offering reactive services such as incident triage, incident coordination artifact analysis and incident resolution.

5.1.1 *Incident Triage*

G-SIRT handles triage verifying the reliability of the source and finding any other valuable information. G-SIRT determining if an incident is authentic, assessing and prioritizing the incident.

5.1.2 *Incident Coordination*

G-SIRT coordinates incident management acting as described following:

1) Identifying constituency parties involved (owned company, internal department/office or team).
2) Establishing contacts with all the stakeholders in order to analyze the incident and identify actions to be undertaken.
3) Facilitating contacts with other involved parties that can provide support for solving the incident.
4) Promptly informing company's management at the level corresponding to incident severity;
5) Writing reports and share it to other CERTs or interested organizations.

5.1.3 *Incident Resolution*

G-SIRT defines containment strategies, suggests and coordinates actions to contrast incidents in order to ensure normal operations conditions as quickly as possible.

5.2 Proactive Services

5.2.1 *Security Announcements*

G-SIRT provides information needed to protect Grimaldi Group's information assets aiming to:

- Disseminate useful information for the growth of cyber security awareness of its constituency.
- Publish announcements concerning security threats relevant for its constituency.
- Provide and promote information exchange within peers and its constituency;

5.2.2 *Security Assessment*

G-SIRT reviews and analyses the security infrastructure, based on the requirements defined by Grimaldi Group that apply. Furthermore an infrastructure Risk Analysis methodology was established

aligned with organization security requirements.

G-SIRT security assessment includes:

- Infrastructure review: a semiautomatic review is performed on hardware and software configuration, router, firewall, servers and desktop devices to ensure that they match the organizational and industry best practices, security policies and standard configurations.
- Scanning: a vulnerability scanning is performed periodically (quarterly) to determine which systems and networks are vulnerable. All vulnerabilities linked to a risk level out of risk acceptance area, will be addressed with an appropriate response.

6 - INCIDENT REPORTING FORMS

All constituency members could report an incident via email to G-SIRT email address.

In this case, it is necessary to provide as much more information as possible, such as:

- Date/time of event;
- Brief event description
- Involved actor or system (even potentially involved)
- Other.

Do not send malicious code or other attachments via email without having previously agreed with a G-SIRT team members.

7 - DISCLAIMER

G-SIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.