ISO 27001
ISO 22301
ISO 9001

BUREAU VERITAS
Certification

cipher
a PROSEGUR company

CIPHER-CSIRT

RFC2350

TLP:WHITE

Table of Contents

1 Document Information

1.1 Abstract

This document describes the CIPHER-CSIRT, the Cipher CSIRT team, according to RFC 2350. The RFC 2350 is an RFC (Request for Comments) which describes the structure, the procedures and the policies of a CSIRT (Computer Security Incident Response Team). The RFC 2350 can be downloaded from http://www.ietf.org/rfc/rfc2350.txt.

1.2 Document Version and last update

This is document version 2.1, published May 12th, 2022.

1.3 Locations where this document can be found

The current version of this document is available from the CIPHER-CSIRT site:

https://www.cipher.com/irt/rfc/

There are three documents in Portuguese, Spanish and English of this document.

You also have the option of reading it in two formats: PDF and TXT.

1.4 Locations where this document can be found

This document has been signed with CIPHER-CSIRT PGP key. The signature is also available at: https://www.cipher.com/irt/rfc

2 Contact Information

2.1 Name of the Team

CIPHER-CSIRT: the Cipher Computer Security Incident Response Team.

2.2 Address

Cipher Portugal: Rua do Brasil 239 - Coimbra 3030-175 - Portugal

2.3 Time Zone

Portugal/WEST (GMT+0 and GMT+1 from April to October).

2.4 Telephone Number

+351 239 047 756

2.5 Electronic Mail Address

irt@cipher.com

2.6 Public Keys and Other Encryption Information

The CIPHER-CSIRT has a PGP key for secure communication.

CIPHER-CSIRT: irt@cipher.com

Fingerprint: 4DDB281530FE5EBF0A0CB25FBC2FF8B2117AD4BA

2.7 Team Members

(Ordered alphabetically)

Alexandre Fernandes - ajfernandes@cipher.com

Antonio Javier Montes Ortega - antonio-javier.montes@prosegur.com

Antonio Manuel de Jesus Ribeiro - aribeiro@cipher.com

João Dias - jdias@cipher.com

Jorge Hurtado Rojo – Jorge.hurtado@prosegur.com

Yaser Rimawi – yaser.rimawi@prosegur.com

2.8 Other Information

Information regarding activities and structure of the CIPHER-CSIRT, as well as links to various recommended security resources can be found at http://www.cipher.com/irt/

2.9 Points of Customer Contact

The preferred method for contacting CIPHER-CSIRT is via e-mail at irt@cipher.com. If it is not possible (or not advisable for security reasons) to use e-mail, the CIPHER-CSIRT can be reached by telephone at +351 239 047 756 during regular office hours.

3 Charter

3.1 Mission Statement

The purpose of the CIPHER-CSIRT is to respond to security incidents in its own infrastructure as well as its client's infrastructure, assuring a high degree of availability and the business continuity of affected clients.

3.2 Constituency

The CIPHER-CSIRT constituency is its own infrastructure as well as the infrastructure of its clients. Currently the following IP addresses are part of our constituency:

193.126.27.160/27	195.23.143.234 /32	195.23.224.98 /32
40.67.248.173/32	195.23.60.129 /32	195.23.224.106 /32
20.107.147.189/32	195.23.143.227 /32	195.23.143.249 /32
82.154.252.14 /32	195.23.143.229 /32	195.23.224.105 /32
195.23.224.96 /32	195.23.143.240 /32	195.23.144.175 /32
195.23.143.250 /32	195.23.143.241 /32	195.23.137.100 /32
195.23.60.218 /32	195.23.93.145 /32	195.23.137.168 /32
195.23.29.246 /32	195.23.143.236 /32	195.23.22.54/32
195.23.143.228 /32	195.23.143.242 /32	41.76.144.0/24
195.23.224.100 /32	78.130.38.48 /32	41.76.145.0/24
195.23.60.124 /32	195.23.143.244 /32	197.235.1.0/24
193.126.251.153 /32	195.23.143.245 /32	197.235.2.0/24
193.126.251.150 /32	195.23.143.246 /32	197.235.3.0/24
193.126.251.149 /32	195.23.143.247 /32	197.235.4.0/24
193.126.251.156 /32	195.23.143.248 /32	41.140.246.146/31
193.126.251.155 /32	195.23.60.123 /32	102.50.241.42/32
193.126.251.154 /32	195.23.143.230 /32	102.50.241.28/32
193.126.251.152 /32	195.23.224.97 /32	102.176.248.0/24
195.23.224.103 /32	195.23.143.237 /32	89.115.243.16/28
195.23.224.99 /32	195.23.143.238 /32	136.144.172.28/32
195.23.60.127 /32	195.23.60.128 /32	196.13.101.0/24
195.23.143.231 /32	195.23.143.239 /32	41.94.97.128/28
195.23.143.232 /32	195.23.60.126 /32	105.235.217.0/29
195.23.156.64 /32	195.23.224.104 /32	197.219.208.182/32
83.240.180.80/29	62.28.4.226/32	

3.3 Authority

The CIPHER-CSIRT expects to work cooperatively with the system administrators and users of the client infrastructures, in so far as possible, to assure the necessary authority to respond to security incidents.

4 Policies

4.1 Types of Incidents and Level of Support

The CIPHER-CSIRT restricts its support and incident handling to incidents that fall under its constituency.

The following list represents the type of incidents to which the CIPHER-CSIRT will provide support.

The following list follows the common taxonomy used by the National CSIRT network[1] of which the CIPHER-CSIRT was founding member and is still member.

- Computer forgery - Intentional act of introducing, modifying, deleting or suppressing of computer data, or by any other way interfering with the functioning of a computer system without right, resulting in inauthentic data or documents, with the intent that it be considered or acted upon for legal purposes as if it were authentic. Includes the use of phishing web sites for credential theft and the distribution of phishing emails.
- Computer system interference - Intentional action or attempt to prevent or gravely disrupting the functioning of a computer system by introducing, transmiting, damaging, deleting, deteriorating, alterating, suppressing or rendering inaccessible any software component or hardware without right. Includes denial of service attacks.
- Illegal access to a computer system - Intentional access or attempt to the whole or any part of a computer system without right. Includes the theft of information, namely business secret, industrial secret or confidential data protected by statute.
- Data interference - Intentional act or attempt to delete, damage, deteriorate, alterate, suppresse or render inaccessible computer data without right. Includes malware and its distribution by email.
- Unauthorized gathering of data - Intentional act of gathering information about networks and computer systems without right.
- Copyright infringement - Copyright infringement, regardless of its content being information, source code, graphical projects or any other elements of computer systems protected by copyrights.
- Unsolicited electronic mail - Unsolicited reception/sending of e-mail, whether produced for direct marketing purposes ou with no aparent purpose. Malware distribution or phishing attacks are not included.
- Other security infringement - Other infringement to the IT security policy.

Under normal conditions the CIPHER-CSIRT will reply to any of the above described incidents within 24 hours.

4.2 Co-operation, Interaction and Disclosure of Information

The CIPHER-CSIRT applies to the information that manages the protection measures corresponding to its nature and classification, taking as a reference, among others, the General European Data Protection Regulation (GDPR) and the European NIS directive.

[1] https://www.cncs.gov.pt/pt/certpt/index.php/pt/rede-nacional-csirts/documentos/1489-classificacao-de-incidentes

Likewise, in communications and documentation, the FIRST TLP v1.1 protocol is used internally and externally for the classification and labeling of documents, according to which the following levels of information classification have been established:

- RED. Information not distributable and restricted to representatives authorized to participate directly in the exchange of information and who have signed the corresponding confidentiality commitments.
- AMBER. Information of limited and restricted distribution to authorized personnel, belonging to the service or its beneficiary organizations, who have a legitimate need to know in order to exercise their functions, and who have signed the corresponding confidentiality commitments.
- GREEN. Information of limited distribution and restricted to personnel and institutions within the service's trusted network and with which non-distribution agreements are established but cannot be freely published or freely accessible.
- WHITE. Information that is freely distributed and not restricted but that may be subject to Copyright

Information tagged with identifiers in the TLP will be handled accordingly.

When reporting a sensitive incident, please indicate so appropriately, using the appropriate TLP label in the subject line, and please consider using encryption as specified in section 2.6

The CIPHER-CSIRT will handle all information it is provided as confidential. However statistical data can be generated from some of this information as long as full confidentiality and anonymization can be ensured.

All confidentiality and privacy customer rights are safeguarded by a non-disclosure agreement which is part of the standard incident handling service contract.

4.3 Communication and Authentication

In view of the types of information that the CIPHER-CSIRT will likely be dealing with, telephones and unencrypted e-mail will be sufficiently secure for low-sensitivity data. Any sensitive data should be encrypted with PGP.

5 Services

5.1 Incident Response

The CIPHER-CSIRT only responds to incidents that affect its constituency and follows the best practices published by entities like CERT-CC, ENISA, Trusted Introducer and FIRST.

5.2 Incident Triage

This stage will prioritize incidents according to an initial analysis which will take into account the type of incident, impact, extent, and other characteristics. All incidents will be assigned a unique identifier.

5.3 Incident Coordination

The analysis and investigation of an incident will identify the root causes of the incident and if needed the involved entities or persons will be contacted. If the incident is outside the scope of action of the CIPHER-CSIRT the information will be forwarded to the responsible entity.

5.4 Incident Resolution

This includes providing guidance and support to resolve the incident, and secure the system, as well as collecting evidence where criminal prosecution, or disciplinary action, is contemplated.

The incident is considered to be resolved when all affected system have resumed normal operation.

Non-confidential data can be gathered to generate statistical information or if needed to report to other involved CSIRT.

5.5 Proactive Activities

The CIPHER-CSIRT provides consulting services. Detailed descriptions of these services are available at: https://www.cipher.com

6 Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, CIPHER-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained within.

Furthermore, several contractual obligations are included in the standard service contract, which only cover the involved parties.

cipher
a PROSEGUR company

SPAIN

Madrid
Calle Juan Ignacio Luca de Tena, 6
Madrid, 28027
Phone **+34 915 898 100**

Barcelona
Av. Gran Vía Hospitalet 175
Barcelona, 08908

UNITED KINGDOM

2 Kingdom Street
London, W2 6BD
United Kingdom
Phone: **+44 203 580 4321**

PORTUGAL

Lisbon
Av. Infante D. Henrique 326
Lisbon, 1849-006

Coimbra
Rua do Brasil 239
Coimbra, 3030-175
Phone **+34 915 898 100**

USA

1111 Brickell Avenue
Miami, FL 33131
United States
Phone:**+1 305 373 4660**

BRAZIL

São Paulo
Rua Alexandre Dumas 1658
São Paulo, 04717-004
Phone: ***+55 11 4501 6600***

Rio de Janeiro
Praça 15 de Novembro 20
Rio de Janeiro, 20010-010

COLOMBIA

Transversal 23 #95 - 53
Bogota, 110221

Email **irt@cipher.com**