-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

RFC 2350: RCTS CERT

Last Revision: Carlos Friaças

1 Information about this document

1.1 Last update date

Version 3.3 published on 2020/06/07.

1.2 Distribution lists for notifications

There is no distribution channel to notify changes on this document.

1.3 Access to this document

The updated version of this document can be found at

+ http://www.cert.rcts.pt/images/docs/RFC2350RCTSCERT_EN.pdf

A Portuguese version can be found at

+ http://www.cert.rcts.pt/images/docs/RFC2350RCTSCERT.pdf

1.4 Authenticity of this document

This version of RCTS CERT's service description is signed with RCTS CERT's PGP key.

2 Contact information

2.1 Team Name

RCTS CERT

2.2 Postal Address

Fundação para a Ciência e a Tecnologia
Unidade de Computação Científica Nacional
RCTS CERT
Apartado 50435
1700-001 Lisboa
Portugal

2.3 Time zone

Portugal/WEST (GMT+0, GMT+1 during summertime)

2.4 Phone Number

+351 218 440 177

2.5 Fax

+351 218 440 185

2.6 E-mail

report@cert.rcts.pt; info@cert.rcts.pt; seguranca@fccn.pt; cert@cert.rcts.pt; security@cert.rcts.pt; abuse@cert.rcts.pt

2.7 Other Types of Telecommunications

Nonexistent.

2.8 Public Keys and Encryption Information

RCTS CERT's PGP key has *KeyID* 0x763EF298 and its *fingerprint* is F96E A4BB 0892 B45E 8DA6 E83B 071D CCEB 763E F298. This key can be found at the usual key servers on the Internet such as pgp.mit.edu or pool.sks-keyservers.net.

2.9 Team Members

Coordination: Carlos Friaças
Members: Helder Fernandes, Filipa Macieira, Miguel Rosa, Yevgen Goncharuk
Legal advice: Miguel Andrade

2.10 Further Information

Further information about RCTS CERT can be found at http://www.cert.rcts.pt/.
Team info is also available at:
+ https://www.trusted-introducer.org/directory/teams/rcts-cert.html
+ https://www.first.org/members/teams/rcts_cert

2.11 Types of contact for users

RCTS CERT has the following types of contact (in order of preference):

E-mail for reporting security incidents:

report@cert.rcts.pt; cert@cert.rcts.pt; seguranca@fccn.pt

E-mail for other related issues with computer security:

info@cert.rcts.pt; security@cert.rcts.pt

Phone

+351 218 440 177

Fax

+351 218 440 185

3 Charter

3.1 Mission Statement

RCTS CERT's central mission is contributing to the cybersecurity effort from user communities tied to organizations connected to the Science, Technology and Society Network (RCTS), namely through

processing and coordination of incident response, by producing security alerts and recommendations, and to promote a security culture.

3.2 Constituency

RCTS CERT provides incident handling on RCTS' (Science, Technology and Society Network) user community context. IP address ranges within RCTS CERT's scope are:

2001:690::/32
139.83.0.0/16
158.162.0.0/18
158.162.64.0/19
158.162.96.0/20
158.162.112.0/21
158.162.128.0/18
185.175.184.0/22
192.26.231.0/24
192.26.236.0/24
192.67.76.0/24
192.68.186.0/24
192.68.209.0/24
192.68.216.0/24
192.68.221.0/24
192.68.224.0/24
192.76.242.0/24
192.80.20.0/24
192.82.127.0/24
192.84.13.0/24
192.84.15.0/24
192.86.138.0/24
192.88.17.0/24
192.88.250.0/23
192.88.252.0/23
192.88.254.0/24
192.92.133.0/24
192.92.142.0/24
192.92.144.0/24
192.92.145.0/24
192.92.146.0/24
192.92.147.0/24
192.92.148.0/24
192.92.149.0/24
192.92.152.0/24
192.92.153.0/24
192.104.48.0/24
192.107.122.0/24
192.122.238.0/23
192.122.240.0/23
192.122.242.0/24
192.132.53.0/24
192.132.55.0/24
192.135.187.0/24

192.135.219.0/24
192.136.52.0/24
192.138.86.0/24
192.138.204.0/24
192.190.174.0/24
192.195.195.0/24
193.136.0.0/15
193.236.100.0/23
193.236.160.0/20
194.117.0.0/20
194.117.16.0/21
194.117.40.0/21
194.117.48.0/23
194.210.0.0/16

Incident handling is RCTS CERT's responsibility, on the terms foreseen at the "Medidas de Controlo de Incidentes de Segurança Informática" document (http://www.cert.rcts.pt/images/docs/medidas_de_controlo_de_incidentes_de_seguranca_informatica.pdf), specifically regarding feedback timeframes, incident types, communication means and traffic control measures contained within.

3.3 Affiliation

RCTS CERT is a service component of RCTS – Rede Ciência, Tecnologia e Sociedade:

+ https://www.fccn.pt/en/institutional/rcts/

RCTS CERT is a founding member of the National CSIRT Network:

+ https://www.redecsirt.pt/#membros

RCTS CERT is a certified member of TF-CSIRT:

+ https://www.trusted-introducer.org/directory/teams/rcts-cert.html

RCTS CERT is a full member at FIRST:

+ https://www.first.org/members/teams/rcts_cert

RCTS CERT is part of ENISA's CERT inventory:

+ https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe/
+ https:// www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

3.4 Authority

RCTS CERT is a service component of RCTS - Rede Ciência, Tecnologia e Sociedade. Its authority is defined on the RCTS User Letter (https://www.fccn.pt/wp-content/uploads/2016/07/RCTS_AUP.pdf [Portuguese version only]), specifically on:

(Translated)
Failure to comply
1. FCT|FCCN's Board will analyze, on a case-by-case basis, any complaints about non-compliance with the provisions of this document. In the event such complaints are

validated, entities involved will be notified and should immediately fix their situation. If this isn't the case entities can then be disconnected from RCTS.
2. In extreme situations, and with the goal of avoiding more significant damages, the Board can, unilaterally, decide to temporarily disconnect a single or collective person. In those occasions, FCT|FCCN will take all efforts possible to warn involved entities before the disconnection occurs, and reestablishing the connection when it is considered safe.
3. When a connection is unilaterally deactivated, FCT|FCCN undertakes itself to send, in a maximum of three days, by fax or express mail, a fully detailed technical report.

4 Policies

4.1 Incident types and support level

RCTS CERT handles all types of security incidents, and has adopted the Portuguese National CSIRT Network Taxonomy, available at: https://www.redecsirt.pt/files/Taxonomiav2.5.pdf

4.2 Cooperation, interaction and privacy policy

RCTS CERT's privacy policy and data protection establishes that sensitive information can be sent to third parties, only and exclusively on a real need basis and with express previous authorization from the individual or organization to which that information regards to.

4.3 Communication and authentication

From the communication means made available by RCTS CERT, phone and non-ciphered e-mail are considered to be sufficient to non-sensitive information transmission. In order to transmit sensitive information, PGP usage is mandatory.

5 Services

5.1 Handling of security incidents

Security incident handling is RCTS CERT's main service. A security incident is any action or set of actions developed against a compute or network of computers, which results, or can result, in a loss of confidentiality, integrity or performance of a data network or digital system, namely non-authorized access, modification or removal of information, interference or service denial in a digital system. RCTS CERT handles security incidents in the context of RCTS - Rede Ciência, Tecnologia e Sociedade – incidents which source or target of an attack is within RCTS.

5.2 Alert dissemination

RCTS CERT aims to gather a set of information received from several well-known sources, evaluate its severity degree and translate it to Portuguese language. Depending on the severity degree, the analyzed information can result in a security alert, on a recommendation or a simple news entry published on the http://www.cert.rcts.pt/ portal.

5.3 New CSIRT teams support

RCTS CERT also intends to promote the creation of new security incident handling teams within RCTS and in the Portuguese Public Administration context. This service includes holding training events

directed to security incident handling, spreading the word about the theme on adequate fora, and the support to the creation of new CSIRTs.

5.4 DNS Firewall

RCTS CERT makes available to its constituency a DNS-based mechanism that prevents communications with malicious domains. The service encompasses the maintenance and dissemination of a list of malicious domains. In the event that a user accesses a URL that contains a malicious domain, the content displayed will be a local page, indicating that the URL that you tried to access includes malicious content.

5.5 Security Audits

Security audits are performed on request, strictly for RCTS CERT's constituency. Each audit involves the preparation of a report containing the set of facts found and also suggestions for mitigation.

5.6 Monitoring against *web defacements*

Alarms against web defacements is a RCTS CERT pilot service, which includes continuous monitoring, archiving several versions of a web server to be able to register/evaluate any changes. This service is only available for the constituency.

5.7 Anti-Phishing awareness campaigns

RCTS CERT develops on-demand phishing campaigns for members of its constituency and other organisations that sign a specific agreement. Following the development of a campaign, there will also be an awareness session addressed to the set of people defined as the target group. The aim of this service is to provide a tool to evaluate the degree of exposure of an organization to potential future incidents, increasing awareness to cybersecurity issues.

5.8 Intrusion Detection

Intrusion detection for RCTS connected organisations is a service in development. The aim of this service is to eliminate the lack of intrusion detection mechanisms within members' infrastructures. The extension of the current intrusion detection platform will also increase the number of occurrences that will generate external notifications.

6 Disclaimer

While all precautions were taken in the preparation of disclosed information on the Internet portal or through distribution lists, RCTS CERT assumes no responsibility for errors or omissions or for damages resulting from the use of that information.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE+W6kuwiStF6Npug7Bx3M63Y+8pgFAl7dJpsACgkQBx3M63Y+

8pgviw//bYfnEcRasqLUJfNMvjLabPx/r7TXD3IX9HFeITAkkjbba72Xu0TZhYk4
02gZxKKjAbpdEKCYDbth4jZ075MMDuCofxAwXU7GoaICuca0PfsQH3SneBgFlbbe
EVjNOdtBUAg3FyujiWygecrAhyXfSZLQcQgppiOdBYf3+oCtNI7GKcmwstUchfCI
mr5TC+cIxtBW0ehLPKzUa2F6KALmqpOkLmML1G0OT60lkqJUK3MrC/Y0z62JULVB
WYCQVEkTRpXU7/IUgsR49MOiof3itaAaqr3EQZstD0Qf0TtsTpLr+yIoRl+s0+MS
sf1MIG5eIzB4Dpx/fCsgDISCR9DtRc39k1iHxm2CpX2EMRnY9ddWKhWTmCpjnMPH
rG1tpxbuRiqrHZHLqd5gGgxfLw/bbCw1c4JUz6mOtahAKw6m8PKxwl+Rggh8zHrY
PuuMwA0g1LAhmFhMN/f0fuDA9Tn1Qr3jCt8h+XsGkTdtpTPVrwUI25m4olZ3oKzn
W0korr6/bdgedGZY8JC2SpSQmp4JcHtN3LNabYtyfgQTo+QpX8hctZS/xRd7nYHi
dz/KSXJuRpO7sLIWaoslg4lQxhl4116lUwthknpC6CV1JEJa1fPp95sOWusbB0zR
D9bzpAigxkuOZ4OKrhtsMIyj1O2gcAdhdaBIu4rNWP+N/4g89/o=
=K8mF
-----END PGP SIGNATURE-----