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

Hash: SHA256

RFC 2350: RCTS CERT

Última Revisão: Carlos Friaças

1 Informação acerca deste documento

1.1 Data da última atualização

Versão 3.3 publicada em 2020/06/07.

1.2 Listas de distribuição para notificações

Não existe um canal de distribuição para notificar alterações a este documento.

1.3 Acesso a este documento

A versão atualizada deste documento pode ser encontrada em

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

Uma versão atualizada deste documento pode ser encontrada em

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

1.4 Autenticidade deste documento

Esta versão da descrição do RCTS CERT encontra-se assinada com a chave PGP do RCTS CERT.

2 Informação de contacto

2.1 Nome da equipa

RCTS CERT

2.2 Endereço postal

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

2.3 Zona horária

Portugal/WEST (GMT+0, GMT+1 em horário de verão)

2.4 Telefone

+351 218 440 177

2.5 Fax

+351 218 440 185

2.6 Endereço de correio eletrónico

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 Outras telecomunicações

Não existentes.

2.8 Chaves públicas e informação de cifra

A chave PGP do RCTS CERT tem o *KeyID* 0x763EF298 e o *fingerprint* é F96E A4BB 0892 B45E 8DA6 E83B 071D CCEB 763E F298. Esta chave pode ser encontrada nos habituais servidores de chaves públicas existentes na Internet, como por exemplo pgp.mit.edu ou pool.sks-keyservers.net.

2.9 Membros da equipa

Coordenação: Carlos Friaças
Membros: Hélder Fernandes, Filipa Macieira, Miguel Rosa, Yevgen Goncharuk
Apoio jurídico: Miguel Andrade

2.10 Outra informação

Mais informação sobre o RCTS CERT pode ser encontrada em https://www.cert.rcts.pt/.
Informação sobre a equipa está também disponível em:
+ https://www.trusted-introducer.org/directory/teams/rcts-cert.html
+ https://www.first.org/members/teams/rcts_cert

2.11 Meios de contacto para utilizadores

O RCTS CERT dispõe dos seguintes meios de contacto (por ordem de preferência):

Correio eletrónico para comunicação de incidentes de segurança informática:

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

Correio eletrónico para outros assuntos relacionados com segurança informática:

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

Telefone

+351 218 440 177

Fax

+351 218 440 185

3 Guião

3.1 Missão

O RCTS CERT tem como missão central contribuir para o esforço de cibersegurança das comunidades utilizadoras das entidades ligadas à Rede Ciência, Tecnologia e Sociedade (RCTS), nomeadamente

através do tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de cibersegurança.

3.2 Comunidade servida

O RCTS CERT responde a incidentes de segurança informática no contexto da comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade. As gamas de endereços IP abrangidos no âmbito de atuação do RCTS CERT são:

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

É da responsabilidade do RCTS CERT o tratamento de incidentes para a RCTS, nos termos previstos no documento "Medidas de Controlo de Incidentes Segurança Informática" (http://www.cert.rcts.pt/images/docs/medidas_de_controlo_de_incidentes_de_seguranca_informatica.pdf), designadamente em observância dos tempos de resposta, tipos de incidente, meios de comunicação e medidas de controlo de tráfego nele constantes.

3.3 Filiação

O RCTS CERT é um serviço integrante da RCTS – Rede Ciência, Tecnologia e Sociedade:

+ https://www.fccn.pt/institucional/rcts/

É membro fundador da Rede Nacional de CSIRT:

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

É membro certificado da TF-CSIRT:

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

É membro de pleno direito do FIRST:

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

É um CERT integrante do inventário de CERTs da ENISA:

+ 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 Autoridade

O RCTS CERT é um serviço integrante da RCTS - Rede Ciência, Tecnologia e Sociedade. A sua autoridade encontra-se definida na carta do utilizador da RCTS (https://www.fccn.pt/wp-content/uploads/2016/07/RCTS_AUP.pdf), designadamente no disposto em:

> ***Incumprimento***
> *1. Conselho Executivo da FCT|FCCN analisará, casuisticamente, eventuais denúncias sobre o incumprimento do preceituado neste documento. No caso de estas terem*

procedência, as entidades envolvidas serão notificadas devendo, de imediato, regularizar a sua situação sob pena de serem desligadas da RCTS.
2. Em casos extremos, e com o fim de evitar danos maiores, o Conselho Executivo poderá, unilateralmente, decidir desligar temporariamente uma pessoa singular ou colectiva. Em tais situações, a FCT|FCCN fará todos esforços para avisar as entidades envolvidas antes da desconexão, restabelecendo a ligação assim que esta seja considerada segura.
3. Sempre que uma ligação seja desactivada unilateralmente, a FCT|FCCN compromete-se a enviar, no prazo máximo de três dias, via fax ou correio expresso, um relatório técnico explicativo devidamente fundamentado.

4 Políticas

4.1 Tipos de incidente e nível de suporte

O RCTS CERT responde a todos os tipos de incidente de segurança, sendo que adota a taxonomia da Rede Nacional CSIRT, disponível em: https://www.redecsirt.pt/files/Taxonomiav2.5.pdf

4.2 Cooperação, interação e política de privacidade

A política de privacidade e proteção de dados do RCTS CERT estabelece que informação sensível pode ser transmitida a terceiros, única e exclusivamente em caso de real necessidade e com a autorização prévia expressa do indivíduo ou entidade a quem essa informação diga respeito.

4.3 Comunicação e autenticação

Dos meios de comunicação disponibilizados pelo RCTS CERT, o telefone e o mail não cifrado são considerados suficientes para a transmissão de informação não sensível. Para a transmissão de informação sensível é obrigatório o uso de cifra PGP.

5 Serviços

5.1 Tratamento de incidentes de segurança

O tratamento de incidentes de segurança informática configura o principal serviço do RCTS CERT.
Entende-se por incidente de segurança informática qualquer ação ou conjunto de ações desenvolvidas contra um computador ou rede de computadores e que resulta, ou pode resultar, na perda da confidencialidade, integridade ou desempenho de uma rede de comunicação de dados ou sistema informático, designadamente, o acesso não autorizado, a alteração ou remoção de informação, a interferência ou a negação de serviço em sistema informático. O RCTS CERT trata incidentes de segurança informática no contexto da comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade, ou seja, incidentes onde a origem ou o alvo dos ataques é a RCTS.

5.2 Disseminação de alertas

O RCTS CERT propõe-se reunir um conjunto de informação recebida de várias fontes bem conhecidas, avaliar o grau de severidade e traduzi-la para língua portuguesa. Dependendo do seu grau de severidade a informação analisada pode resultar num alerta de segurança, numa recomendação ou numa simples notícia publicada no portal http://www.cert.rcts.pt/.

5.3 Apoio à criação de novas equipas de CSIRT

O RCTS CERT tem ainda um serviço de promoção à criação de novas equipas de resposta a incidentes de segurança informática na RCTS e no âmbito da Administração Pública. Este serviço inclui a realização de ações de formação subordinadas à temática da resposta a incidentes, a divulgação do tema nos fora adequados e o apoio à criação de novos CSIRT.

5.4 DNS Firewall

O RCTS CERT disponibiliza para a sua *constituency* um mecanismo baseado no DNS que impede as comunicações com domínios maliciosos. O serviço engloba a manutenção e disseminação de uma lista de domínios considerados como maliciosos. Na circunstância de um utilizador aceder a um URL que contenha um domínio malicioso, o conteúdo apresentado será uma página local, indicando que o URL a que tentou aceder inclui conteúdo malicioso.

5.5 Auditorias de segurança

Auditorias de segurança são realizadas a pedido, estritamente para os membros da *constituency* do RCTS CERT. Cada auditoria pressupõe a elaboração de um relatório contendo os factos encontrados e também sugestões de mitigação.

5.6 Monitorização contra *web defacements*

A alarmística contra *web defacements* é um serviço piloto do RCTS CERT, que compreende a monitorização contínua, arquivando diversas versões de um servidor *web* para ser possível registar/avaliar eventuais alterações. Este serviço está apenas disponível para a *constituency*.

5.7 Campanhas de *awareness* Anti-Phishing

O RCTS CERT desenvolve campanhas de *phishing* a pedido para membros da sua *constituency* e outras entidades protocoladas. Na sequência do desenvolvimento de uma campanha, acontecerá também uma sessão de *awareness* dirigida ao conjunto de pessoas definido como o grupo-alvo. Pretende-se com este serviço disponibilizar uma ferramenta para se avaliar o grau de exposição de uma organização a potenciais futuros incidentes, aumentando o grau de sensibilização de todos para as questões da cibersegurança.

5.8 Detecção de intrusões

A detecção de intrusões no plano da RCTS é um serviço em desenvolvimento. Pretende-se com este serviço colmatar a inexistência de mecanismos de detecção de intrusões em infraestruturas de membros da *constituency* do RCTS CERT. O alargamento da actual plataforma de detecção de intrusões irá permitir também alargar o número de ocorrências que irão gerar notificações externas.

6 Salvaguarda de responsabilidade

Embora todas as precauções sejam tomadas na preparação da informação divulgada quer no portal Internet, quer através das listas de distribuição, o RCTS CERT não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.

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

iQIzBAEBCAAdFiEE+W6kuwiStF6Npug7Bx3M63Y+8pgFAl7dJZIACgkQBx3M63Y+
8pizWA//eArAPyQsH+IAAf/foqh+68oS8UxrBNFgJex5PDsyc6Ucx98pO8bWW86d
uYUuOnStmUtt3EHeCK56XGQEuF9TTUoReHthGYXLAI7L8iQo/pXQrC0TmbwQNO22
/yOYRXYNSAHjWariwvU9xV5o1p34rNf/qZcZ1S7i1ftfTt5Swhahx0thq72bwMko
+ulL8Sm/D0oJeSug+tMMyDNczrRJeQvULdaShFnXEgSXoaDCjOH02rUAujSUXNZ0
GfTZMs1HLUFC15RjUNqgiEztllBhij1NkLuonLJrw0ZcXOEgAWIn199GueEO+LEq
ivAtb+DEu8YHrDM5KBjUOYFv5axAuw6ebZE9FODpLxI+C/c4nDipcvlfHDFTiWL5
9xUZxYTfWh/wU+brGvMwLJttm0aOLIYNEJjZChe1zoe1TPIY56oRDcERtEdLmwq8
6h0/kxP6+94Zo3UQffU8AKpKOoSyGLk0O5AgpSbEDs5WS9OZ15vGBDdLc7v8N3xh
Z6d1sRFmXzvBxSSvClYUNexIJB+kaQFFPkxzlkG9825jPL61X6PPQsjFSAIww1uD
Tkd+DqFHn/79FxTya6tfF040LtuF145MbPhxqM6I1kj3d1uQ41bWkYlynNR2oUBg
JRMggUJxoCo0Zh0i4gXEVgvlf09hbO/ZGPpRqfJmSUVepoQPBUY=
=4kQF
-----END PGP SIGNATURE-----