RFC2350 PT

Data: 18 Dezembro 2019

Versão: 1.4

Refª: WRP192406

Índice

1. Informação acerca deste documento

Este documento descreve os serviços de resposta a incidentes de segurança informática da Warpcom Services, de acordo com a RFC2350 disponibilizado publicamente em http://www.ietf.org/rfc/rfc2350.txt.

A Warpcom Services é uma Empresa Nacional Portuguesa, localizada nas cidades de Lisboa, Porto e Madrid.

Todos os documentos possuem uma identificação do documento com data que foram criados e as posteriores datas em que sofreram alterações com a respetiva repercussão na versão.

1.1. Data da última atualização

Versão 1.4, data da última alteração a 2019/12/18

Versão 1.3, data da última alteração a 2019/09/25

Versão 1.2, data da última alteração a 2019/09/23

Versão 1.1, data da última alteração a 2019/06/24

Versão 1.0, data de criação a 2019/06/19

1.2. Listas de distribuição para notificações

Existem 1 (um) endereço de distribuição do qual estão associados aos grupos afetos aos serviços de NOC e SOC sendo ele:

csirt@warpcom.com

1.3. Acesso a este documento

Para fins de validação, uma versão ASCII assinada com PGP está disponível em https://warpcom.com/wp-content/uploads/2019/12/Warpcom-Services-RFC2350-v1.4.txt .

A chave PGP utilizada para assinar é da Warpcom e está disponível no ponto 2. correspondente.

Todos os documentos estão classificados como “Informação pública” quando partilhados no site da Warpcom, “Confidencial” ou “uso interno” quando tratado por os grupos afetos internamente e de acordo com o conteúdo e classificação da informação.

2. Informação de contacto

2.1. Nome da equipa

Name of the CSIRT	CSIRT - Computer Security Incident Response Team da Warpcom

2.2. Endereço postal

Mailing Address	CSIRT - Estrada de Alfragide, 67 Edifício F, Piso 3, Alfrapark 2610-008 Amadora Portugal

2.3. Zona horária

Time zone	Europe/Lisbon GMT +0 ou em horário de verão GMT +1

2.4. Telefone

Telephone number	"+351" 214 169 500

2.5. Fax

Facsimile number	"+351" 214 169 518

2.6. Outras telecomunicações

Não existentes.

2.7. Endereços de correio eletrónico

Correio eletrónico para notificação de incidentes de cibersegurança:

csirt@warpcom.com

Correio eletrónico para assuntos relacionados com os serviços de NOC e SOC da Warpcom CSIRT:

soc@Warpcom.com

noc@Warpcom.com

Correio eletrónico para assuntos gerais e esclarecimentos:

geral@warpcom.com

2.8. Chaves públicas e informação de cifra

Public keys and encryption	User ID: CSIRT <csirt@warpcom.com>
	Key ID: 0x5837B046
	Key type: RSA
	Key size: 4096
	Expires: 11/11/2021
	Fingerprint (256 bits): 4D8E20C22D1DC13898E34CD47D7C16985837B046

A chave está disponível em:

https://warpcom.com/wp-content/uploads/2019/12/Warpcom.csirt-key.txt

```
-----BEGIN CERTIFICATE-----
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBF3JeU0BEAC5zGeMPFoaJ3eKe18ClKu3JDQaENkJcLG87hz+P+Wq5RhT9LmN
6aFTibHsmG3GilA2F4y5R1gYQO9TvNNvnG5dece3yZcfoVKClDE21nsQO7bphVby
6RMbyfwV0Ym0QxFOR7tOL5R/YT5XQFKAGCK125LWs+1r+nG7OwcsY/BjrcmGxPpA
YBVx3pnZrRvEoAPU6zI7UCjdO7HVt+fI1Ob9lAFWDdSBffrtvmcrQgFPHeUCYwHg
Rkigjq7JrsngChiYDqeZGThPikRLU1FO9dffcA1u0af1KmsbFQhiDHzA1WQzd/Us
eyj7s6dBHVKJXjcAkJ/xKmMunZ2IhxThJ6tNWKgoSSsIqhjDV0G89jh2yzoi3JqA
LkAa9jeeldiGaeFoeJ2jo88+Fn1uZ6CY4Q+0lqUShmCwV/LjAQVDNZdtSkpPAFrJ
Y1SH8K5/XSJ01jM0Qyn+otkkMNFd5eLIyGS4NNRxK7sgjN9vScP0Bs2SFw1l3NID
RSRzno/ky/NtmNmKrEh8qTTdDMrHEHVyzpvHhjEtKhOvZXOkfhXzQ/TJgI8G6im/
XtDdnwyEplTG31kr/MCXXeeRkyUE4RXRrQfzD8rndAIhMknpgX5Nv6uhdDZ5VqZT
qHeYWVpySBAzp24DcJGVPMse9t11kCdZUUgfn9Kd2Dfo8qWGC1ycX+IiewARAQAB
tBlDU0lSVCA8Y3NpcnRAd2FycGNvbS5jb20+iQJUBBMBCAA+FiEETY4gwi0dwTiY
40zUfXwWmFg3sEYFAl3JeU0CGyMFCQPDjHMFCwkIBwIGFQoJCAsCBBYCAwECHgEC
F4AACgkQfXwWmFg3sEbeqA//dcgm4gnKTLyLQyGpZ5+zi2ZDxHk6FEJPCc4KMgTK
mP0u6kvj5ILL0Nz/o3coeGU+T92jghLs+bUNfO7bJawM36vX7xH5q2+fvon/grcE
sPGY1nlnMGYhtNZtSyCWjTuhTC5eDRGFtrm09AY3p6IEYAvxLrLBS9rv5lyQAlhL
EOqXoIE9zUlRT/dahpBnodrx0ubQh0Yh6mgw3vAMQBqPrvEhxtBJmnr7OKgzuCnb
E/ULY1g3FhhcegNIrEnVWIzJVZ7ubRg7VuCec4PequmLLzTSUK2PakJD++E2jwAC
h2HkI0vbuocF/+b1YE1BtLdUBp1xkdaNCx9hncg8BKLyKHka0XpBiLQGbxLADhwe
pWC7VBAYTjwKXndWXyViulB67rQ95E3Utw7uUM0FiO6lrdqL0+tYytL91CKtvcZ3
xqHvCksJAiUobYP3TpQPsWeY8YfhheOCfEboMSt2JgV3lc/bTfcnHKoBAMx77ctE
KO7bbWNJ2cwcylw+cuaOuPX6A+yQkEp9Vgpn0sVwN2P9HnDNJu3ZihjoNjriNsPT
6Z7BZ7sDOkSBs3VZdK9j2vKkZPjmhj3GL3nsTyAsaOGp4IbHtB0WG2vMGrjFSISL
D1Qr5reobesRq+IqQl+y19Ym5xuWwLTzl3i81JMVz96SGc7xO7qUJ2jLM0HllW34
bLC5Ag0EXcl5TQEQAKte9LjcdeqRiuZdCnQbN/TbCga9UaAHF5FtTGbrcQmf4uo9
fwtQLht3kVNTVedLNNp+pn5etXkG8o0ss8bLqbJo/qdjk52DyZe8hDUJs4huPQMc
YL1o6bu5+fWh4gnjnad33dCL9+CKC/1INyz/AlJK8YEIux4mcFExloR2zvBi4xV0
UWBMD2t5w4/uYSv5XADXcc7MICwKbSpRsao114caCqYOCD1JPKeBXLBWLJclgdJW
vwx7iQIbu8OEZbFeadCIXwa1j4avagsvx25Mo8Qtf6d6e8Q5ai6mazuZs3h9LhYj
670BCFA5M7ktFWTTDEg9aoVZuan6LHuVGE0ABdLUGTud7/ovSITSK6k0d/Y26aEa
xmzhY1EOVoYD9GtpR8L7NQr6v/6ebxT+Lpj2fvyqm2zmh/SCwGHB7qIUb4OHhW1G
chGNt3e8zGwnJp2e2E0Un3EqjyfmruC+TJOkmBJW/lkWlyaGRHvAalwvEYFRQaNS
6OCFBWVZUrUZFrC/38kLVkuzkTIdGJBo4p0u3a240bck2+nnN2O3uy91xBExC3HZ
GGr2RX9M+Vzpy3McljOeEWEY6ehtLt6Hv7Z4tmtVPwtf98SgJfIBg7nlqjc+bfol
Tygf1QisI7oSlyRFNqg6D5X9sRlHFRn8m4EWz2HLKkRR5o1CLfg9X6DxyY3fABEB
AAGJAjwEGAEIACYWIQRNjiDCLR3BOJjjTNR9fBaYWDewRgUCXcl5TQIbDAUJA8OM
cwAKCRB9fBaYWDewRqh7D/0YvfYvX+m0iZ52B1yBu8MRZ9k+yMfxF/ZmmxUBgxqk
fnHiuV/H5Qt4CVbDHFmtDw8x/obIJn+IZ0c8d+wTh0AE3w3soL3Z2OtSGwp9FUIG
IRq1yJBSZJlnB3FYaz6m1BFA9rQO/AFH+o0/hmo04tEtbRJ4bjyyPe3lvs5LzJhR
FI9RG+aEVY2x730sqDXYif/UK2N7kQh2PIOoal+H2AccMmfhXIKsQVXs15nX8enE
JYGg6Un2gYxK7Aq3oPz0NJwv+AlV4K7R22pJVo/9PXF3PKG9Bg/C7hQgW0XzG9Pf
Lxc1jNVbsNxCDlJkgaLbZSbCTKSjjJFRagzI8QOCZI8tR0cFk1ObM+/Cy1Nmo0uL
lDRAvY256romAP01ILPOMeiylUFvNM4OOt1PRmQ8qOWtH0qut+S5YeCZcJdli65L
DRSit/ER+BnpRyJVNxOAvn9UY/XaCxczZYWzZZJpvY1crp+Iiv6tWwlceoH4dfyX
HF+42tathEd6DE3FVSsyUVcmucTaq4HLPQimv/9ewgIWJCdYuFZ5pIu0f5vlkuD8
0NECTAStmgfRjZJgKCI6FeuGQLSdrBrbeX8BMq5suzHs603jfr2stFJRo3KujfvJ
4t1gUajKneOAajryI6+Pld3CUsZRALSSWnAGzjf8IfSy1rKy+Hx+lVch7EEHNc5c
2w==
=RPZY
-----END PGP PUBLIC KEY BLOCK-----
-----END CERTIFICATE-----
```

2.9. Membros da equipa

Coordenação	Paulo Rosa
Membros	André Alberto e
	Pedro Gomes

Operating Hours	8h30-18h30 e para incidentes críticos 24x7

2.10. Outra informação

Mais informação sobre o CSIRT pode ser encontrada em:

https://www.warpcom.com/servicos-tecnologicos/

2.11. Meios de contacto para utilizadores

O CSIRT dispõe dos meios de contacto elencados nas secções 2.2, 2.4 a 2.7.

3. Guião

3.1. Missão

O CSIRT tem como missão assegurar o plano de resposta a incidentes de segurança informática, nomeadamente no tratamento, coordenação e gestão da resposta a incidentes, realização de auditorias e assessments de segurança, produção de alertas e recomendações de segurança.

3.2. Comunidade servida

O plano de resposta a incidentes assenta nas seguintes gamas de endereços IP's sendo eles:

194.79.89.176/28 193.136.112.70/32

89.6.225.8/32

3.3. Filiação

O CSIRT é um serviço de tratamento, coordenação e gestão da resposta a incidentes integrado nos serviços da Warpcom Services.

3.4. Autoridade

O Warpcom CSIRT é uma equipa responsável pela resposta a incidentes de segurança.

4. Políticas

4.1. Tipos de incidente e nível de suporte

O CSIRT responde a todos os tipos de incidentes de cibersegurança tendo um foco nos seguintes:

a) Código Malicioso
b) Disponibilidade
c) Recolha de Informação
d) Tentativa de Intrusão
e) Intrusão
f) Segurança da Informação
g) Conteúdo Abusivo
h) Vulnerável
i) Fraude

O nível de suporte dado por o CSIRT varia consoante a triagem e classificação atribuída bem como a disponibilidade dos recursos por equipa e área afetos.

4.2. Cooperação, interação e política de privacidade

O CSIRT está abrangido por a política de privacidade e proteção de dados da Warpcom Services que prevê que a informação sensível possa ser passada a terceiros, única e exclusivamente em caso de requisito obrigatório das entidades competentes ou com a autorização prévia expressa da entidade ou a título individual de acordo com a associação da informação implícita.

4.3. Comunicação e autenticação

O CSIRT disponibiliza o contacto telefónico e correio eletrónico não cifrado para as comunicações e transmissões da informação não sensível sendo de acordo com o nível de confidencialidade usado posteriormente as transmissões através do uso da cifra PGP.

5. Serviços

5.1. Resposta a Incidentes

O CSIRT realiza o tratamento, coordenação e gestão da resposta a incidentes entre as entidades envolvidas nomeadamente na triagem de notificações de incidentes, análises técnicas e/ou avançadas, realização de auditorias, resolução dos incidentes ou fornecimento de recomendações de mitigação.

5.2. Triagem de Incidentes

O CSIRT efetua uma triagem de incidentes de forma a identificar se o incidente é autêntico ou é um falso positivo ou reincidente.

Se for reincidente confirma periodicamente se o tratamento continua automatizado.

Se for autêntico efetua uma avaliação, automática ou manual, e prioriza o mesmo de acordo com a criticidade.

5.3. Coordenação de Incidentes

O CSIRT efetua a coordenação e gestão da resposta a incidentes através da investigação dos mesmos, tomada de medidas adequadas de forma proactiva, reativa ou informativa, interação com as organizações envolvidas de forma a dar a conhecer os incidentes aos grupos envolvidos por áreas e de ajuda ou através da função de facilitador na resolução dos incidentes.

5.4. Resolução de Incidentes

O CSIRT efetua a resolução de incidentes através da interação com os grupos de administração dos equipamentos moveis, redes, segurança, aplicações e base de dados ao nível das ações mais adequadas a realizar ou diretamente nos sistemas e soluções de controlo quando indigitados para o mesmo.

O CSIRT realiza, quando solicitado ou indigitado, a analise estatística e recolha de dados para investigações mais avançadas.

5.5. Atividades proactivas

O CSIRT realiza auditorias e assessments de segurança de forma proactiva do qual resulta na produção de alertas e recomendações de segurança.

O CSIRT realiza atualizações, configurações, otimizações e manutenções nas soluções de gestão das soluções e sistemas, controlo de segurança e comunicações.

O CSIRT fornece consultoria e acompanha o progresso dos grupos de administração dos equipamentos moveis, redes, segurança, aplicações e base de dados na mitigação das vulnerabilidades identificadas bem como nas campanhas de sensibilização dos seus colaboradores e clientes de forma a reduzir o risco de incidentes.

6. Formulários de reporte de incidentes

Não estão definidos formulários a preencher para o efeito.

7. Salvaguarda de responsabilidade

O CSIRT aplica todas as salvaguardas e prudências necessárias no tratamento e informação disponibilizada nomeadamente no site institucional, listas de distribuição, contactos disponibilizados e métodos de transmissão da informação, no entanto não assume qualquer responsabilidade por erros, omissões, ou danos resultantes do uso indevido dessa informação.

A notificação de incidentes o CSIRT não se substitui à comunicação à autoridade judiciária ou ao órgão de polícia criminal competente para os devidos atos cibercriminais.