RFC 2350: MoRENet CSIRT

Última Revisão: Equipa de Segurança da MoRENet

1. Informação acerca deste documento

1.1. Data da actualização

Versão 1.0 publicada em 2019/06/04

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

- https://cert.morenet.ac.mz/wp-content/uploads/2019/06/RFC-2350_MoRENet.pdf

1.4. Autenticidade deste documento

Esta versão da descrição do MoRENet CSIRT encontra-se assinada com a chave PGP do MoRENet CSIRT.

2. Informação de contacto

2.1. Nome da equipa

MoRENet CSIRT

2.2. Endereço postal

Estrada Naciona nº 1, Km 60
MoRENet CSIRT
Posto Administrativo de Maluana
Distrito de Manhiça
Província de Maputo
Moçambique

2.3. **Zona horária**

Mozambique/Central Africa Time (GMT+2)

2.4. **Telefone**

+258 84 20 69 850

2.5. **Fax**

+258 21 35 28 60

2.6. **Endereço de correio electrónico**

cert@morenet.ac.mz; abuse@morenet.ac.mz; security@morenet.ac.mz

2.7. **Outras telecomunicações**

Não existentes.

2.8. **Chaves públicas e informação de cifra**

A chave PGP do MoRENet CSIRT tem o KeyID 0x5360020E6316A070 e o fingerprint é B915 36E5 39DD 07F3 E0F5 B2DC 5360 020E 6316 A070. Esta chave pode ser encontrada nos habituais servidores de chaves públicas existentes na Internet, como por exemplo pgp.mit.edu, pgp.key-server.io, pgp.circl.lu ou keyserver.mattrude.com

2.9. **Membros da equipa**

Coordenação: Leonel Nhavene

Membros: Gilberto Ngoca, Viegas Cuamba, Algy Adamo,

Apoio jurídico: Gabinete Júridico do Ministério de Ciência e Tecnologia, Ensino Superior e Técnico Profissional.

2.10. **Outra informação**

Mais informação sobre o MoRENet CSIRT pode ser encontrada em https://www.cert.morenet.ac.mz/.

Informação sobre a equipa está também disponível em http://www.morenet.ac.mz/index.php/en/staff

2.11. **Meios de contacto para utilizadores**

O MoRENet CSIRT dispõe dos seguintes meios de contacto (por ordem de preferência):

Correio electrónico para comunicação de incidentes de segurança informática:

cert@morenet.ac.mz;

Correio electrónico para outros assuntos relacionados com segurança informática:

abuse@morenet.ac.mz

Telefone

+258 84 20 69 850

Fax

+258 21 35 28 60

3. **Guião**

3.1. **Missão**

O MoRENet CSIRT tem como missão coordenar a resposta a incidentes de segurança cibernética no seio da comunidade académica e científica nacional, prestar assistência na resolução de incidentes de segurança, disseminar alertas sobre ameaças eminentes, promover o estabelecimento de CSIRT nas instituições beneficiárias, bem como melhorar o conhecimento geral sobre ciber-segurança no seio dos membros.

3.2. **Comunidade servida**

O MoRENet CSIRT responde a incidentes de segurança informática no contexto das instituições beneficiárias dos serviços da Rede de Instituições de Ensino e Investigação -

MoRENet. As gamas de endereços IP abrangidos no âmbito de atuação do MoRENet CSIRT são:

41.94.0.0/16

196.3.96.0/21

196.13.101.0/24

2C0F:F140::/32

3.3. **Filiação**

O MoRENet CSIRT é um serviço da MoRENet:

- https://www.morenet.ac.mz

3.4. **Autoridade**

O MoRENet CSIRT é um serviço da Rede de Instituições de ensino e investigação de Moçambique - MoRENet. A sua autoridade encontra-se definida na Política de Uso Aceitável da MoRENet (https://www.cert.morenet.ac.mz/MoRENet_AUP.pdf), designadamente no disposto em:

Incumprimento

1.1. *A exclusivo critério da MoRENet, esta poderá suspender os serviços ou rescindi-los caso a instituição beneficiária, seus membros ou terceiros a ele vinculados exerçam uma ou mais actividades acima descritas.*

4. **Políticas**

4.1. **Tipos de incidente e nível de suporte**

O MoRENet CSIRT responde a todos os tipos de incidente de segurança e possui sua propria taxonomia, disponível em: https://www.cert.morenet.ac.mz/Taxonomiav1.0.pdf

4.2. **Cooperação, interação e política de privacidade**

A política de privacidade e proteção de dados da MoRENet CSIRT 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 MoRENet CSIRT, 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 MoRENet CSIRT trata incidentes de segurança informática no contexto da comunidade académica e científica beneficiária dos serviços da MoRENet, incidentes onde a origem ou o alvo dos ataques é a MoRENet ou os seus constituintes.

Um incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou redes de computadores que resultam num impacto negativo para uma instituição, se não tratados de forma correcta.

O MoRENet CSIRT classsifica os incidentes de segurança em duas categorias: incidentes internos e incidentes externos. Os externos são os originados fora das redes das instituições membro ou da infra-estrutura de redes da MoRENet e os internos são os originados na rede interna das instituições membros ou na infra-estrutura de redes da MoRENet.

5.2. **Disseminação de alertas**

O MoRENet CSIRT 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 que será partilhada com os constituintes, através de listas de distribuição e na página Internet do MoRENet CSIRT https://cert.morenet.ac.mz/blog/

5.3. **Monitoramento da Rede**

O MoRENet CSIRT serve-se de ferramentas de análise de fluxo (Netflow), MRTGs, sistemas de detecção de Intrusão (IDS), honeypots implantados em vários pontos da sua espinha dorsal para monitorar o tráfego que corre sobre a rede e obter estatísticas e detectar anomalias e uso irregular da rede.

Estas ferramentas permitem o MoRENet CSIRT identificar possíveis ataques e suas características e criar uma base de conhecimento de incidentes que permitem melhorar a capacidade de reação a eventuais ataques.

5.4. **Gestão de Vulnerabilidades**

É uma abordagem pró-activa para gerir a segurança de rede buscando mitigar os riscos de falhas em equipamentos ou aplicativos que possam comprometer os activos de rede.

O MoRENet CSIRT realiza periodicamente varreduras na rede, análise de logs de equipamentos com a finalidade de identificar possíveis vulnerabilidades nos activos instalados na rede, que possam ser exploradas por pessoas mal-intencionadas.

5.5. **Auditorias**

Auditorias de segurança são realizadas na infra-estrutura de rede das instituições beneficiárias dos serviços do MoRENet CSIRT. Visa identificar falhas de segurança resultantes da não observação das normas e boas praticas para implementação de redes locais. A cada auditoria relatórios contendo os problemas identificados e as recomendações para correcção.

5.6. **Detecção externa**

Disponibilizado em colaboração com outros organismos nacionais e internacionais especializados em ciber-segurança, por forma a possibilitar a interacção com os seus sistemas e aumentar a eficácia na prevenção, detecção e mitigação de incidentes de segurança.

5.7. **Promoção de criação de novos CSIRTs**

O MoRENet CSIRT promove o estabelecimento de CSIRTs nas instituições nacionais de Ensino Superior, Ensino Médio Técnico Profissional e Investigação e apoia os CSIRTs estabelecidos através da promoção de encontros para estimular a troca de experiências e acções de colaboração entre estes.

5.8. **Colecta de análises e incidentes**

A coleta, análise e elaboração de relatórios de estatísticas sobre incidentes.

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 MoRENet CSIRT não assume qualquer responsabilidade por erros ou omissões, ou por danos resultantes do uso dessa informação.