CAIS

O Assunto é Heartbleed

Webinar

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Terça-feira, 29/04/2013 – 10:00h

O Assunto é:

Heartbleed.

OpenSSL™
Cryptography and SSL/TLS Toolkit

RNP

Entendendo o Heartbleed

O que é?

Uma vulnerabilidade provocada por um erro de programação na biblioteca OpenSSL.

Quando surgiu?

A falha foi introduzida na versão 1.0.1 do OpenSSL em 14 de março de 2012.

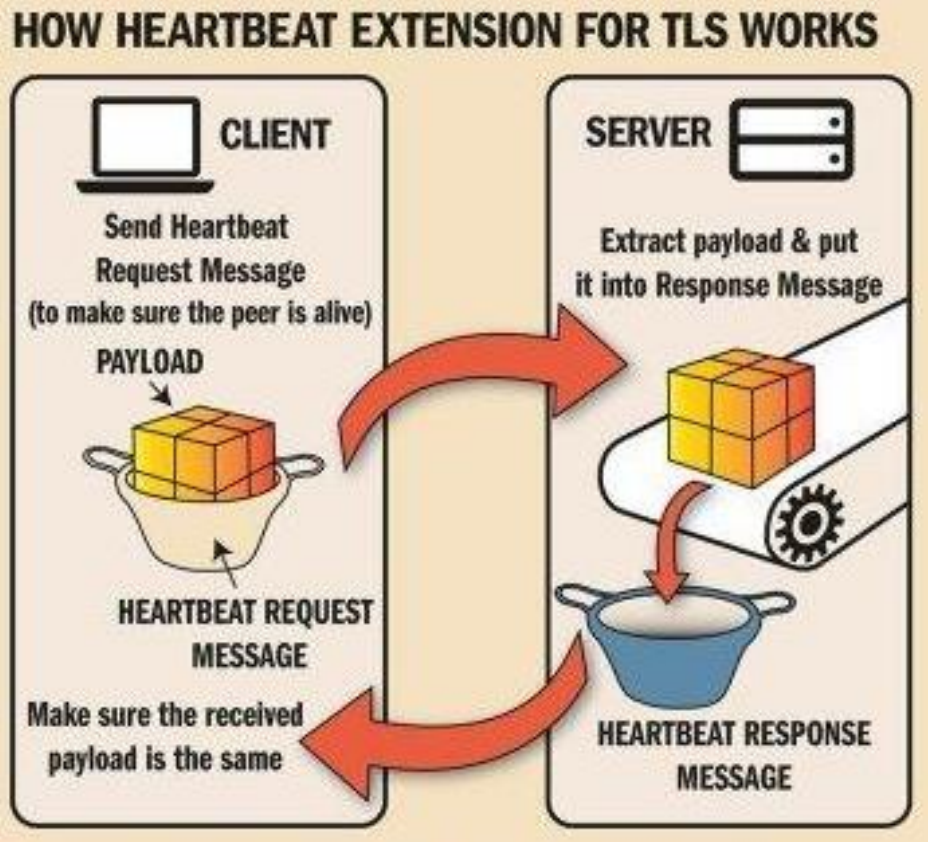
Quando foi divulgado?

No dia 7 de Abril de 2014, totalizando dois anos de existência.

RNP

Entendendo o Heartbeat

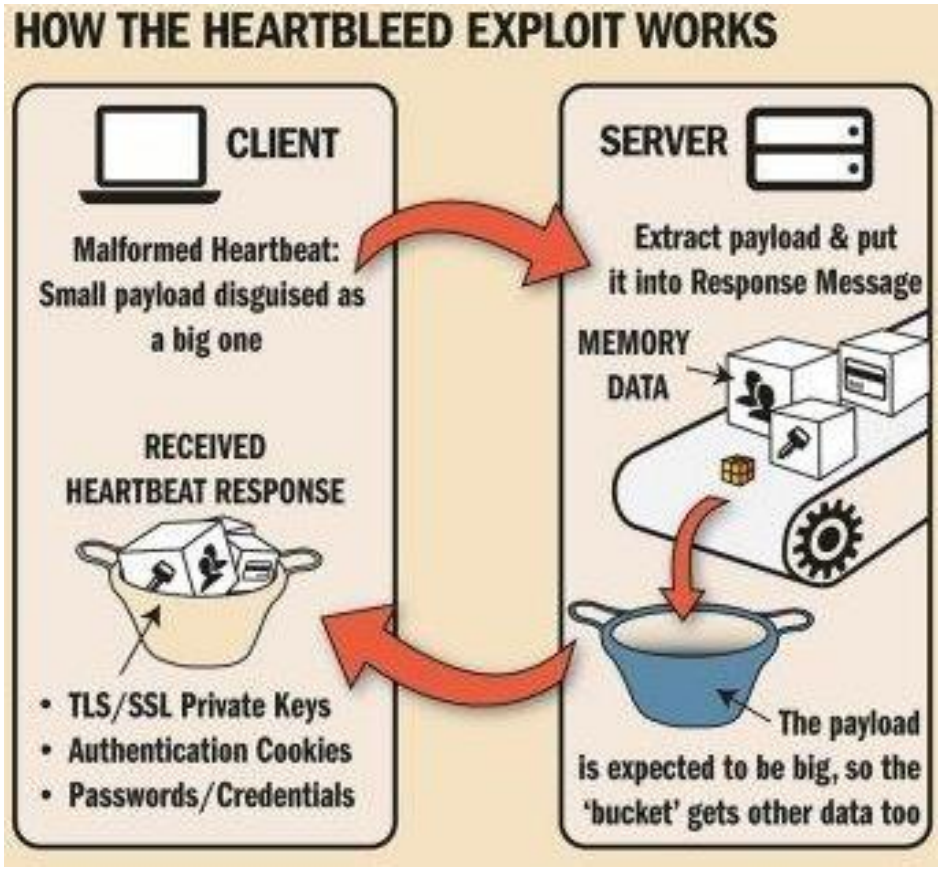
Como funciona?



RNP

Entendendo o Heartbleed

O que ele explora?



RNP

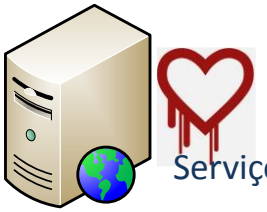
Entendendo o Heartbleed

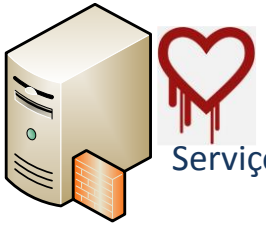
Como funciona?

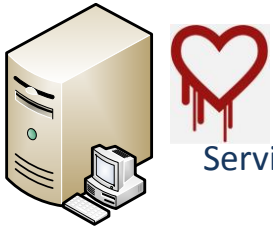
http://xkcd.com/1354/

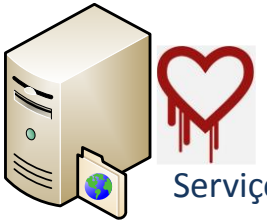
Entendendo o Heartbleed

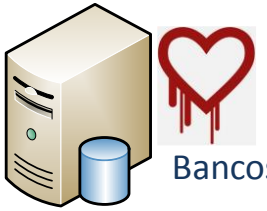
Principais serviços afetados:

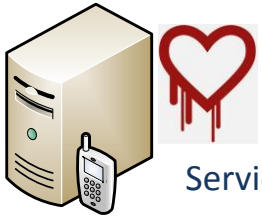

Serviços Web

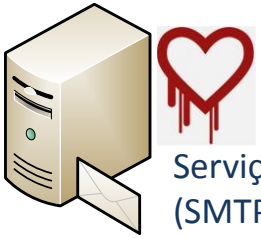

Serviços VPN

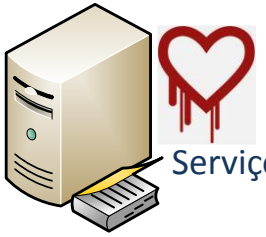

Servidores VMWare

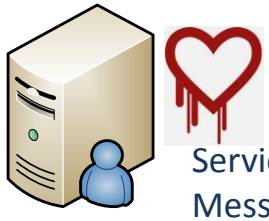

Serviços FTP


Bancos de Dados


Serviços VOIP


Serviços de correio (SMTP, IMAP, POP)


Serviços LDAP


Serviços Instant Messenger

Identificando o Heartbleed

Na Rede Ipê e na RNP:

Rede Ipê:
Cerca de 800 hosts vulneráveis (até o momento).

Principais Ações (Ambiente Corporativo):

- Scans diários para identificação de máquinas vulneráveis
- Atualização de sistemas
- Revogação de certificados digitais e geração de novos
- Troca de senhas dos usuários

RNP

Identificando o Heartbleed

Como saber se estou vulnerável?

- Versões do OpenSSL vulneráveis:
  1.0.1 até 1.0.1f.

- Ferramenta NMAP

- Alguns sites para consulta:
  https://www.ssllabs.com/ssltest/index.html
  https://filippo.io/Heartbleed/

- Smartphones e Tablets também estão vulneráveis

RNP

Identificando o Heartbleed

Como saber se o smartphone ou tablet está vulnerável?

- Sistema Operacional Android versão 4.1.1 é vulnerável
- Aplicativos utilizam sua própria versão do OpenSSL
- Diversos aplicativos na Google Play vulneráveis

RNP

Identificando o Heartbleed

Como saber se o smartphone ou tablet está vulnerável?

AOSP Version	OpenSSL Version	Vulnerable OpenSSL Version	Heartbeats Disabled	Overall Vulnerable
4.4.2_r2	1.0.1e	yes	yes	no
4.4.2_r1	1.0.1e	yes	yes	no
4.4	1.0.1e	yes	yes	no
4.3	1.0.1e	yes	yes	no
4.2.2	1.0.1c	yes	yes	no
4.2	1.0.1c	yes	yes	no
4.1.2	1.0.1c	yes	yes	no
4.1.1	1.0.1c	yes	no	yes
4.0.4	1.0.0e	no	n/a	no

https://bluebox.com/technical/heartbleed-bug-impacts-mobile-devices/

RNP

Resolvendo o Problema

- Atualizar a versão do OpenSSL para 1.0.1g ou mais recente.
- Desabilitar o suporte ao OpenSSL Heartbeat.
- Implementar assinatura no IDS/IPS.
- Utilizar Perfect Forward Secrecy (PFS).
- Recurso adicional de segurança.
  - Empresas que utilizam o PFS: Twitter,Facebook, Microsoft.

http://www.rnp.br/cais/alertas/2014/openssl_1.html

RNP

Resolvendo o Problema

Funcionamento do PFS

- Ambos os hosts criam um par de chaves pública/privada e compartilham as chaves públicas.
- Cada host tem sua própria chave privada a chave pública do outro host.
- Cada host calcula uma chave de sessão compartilhada com a ajuda de sua chave privada e também com a chave pública do outro host.
- A chave de sessão calculada por este método é idêntica nas duas extremidades e, portanto, não há compartilhamento ou transmissão das chaves de sessão.
- Não há compartilhamento das chaves de sessão e as mesmas expiram após pequeno intervalo de tempo.
- Não será possível decifrar um montante de tráfego, visto que, as chaves de sessão foram expiradas.

RNP

Resolvendo o Problema

Tenho como saber se minhas informações foram comprometidas?

Resolvendo o Problema

Demais ações necessárias

- Atualizar firmware dos dispositivos móveis que utilizam Android 4.1.1 Jelly Bean

- Trocar todos os certificados dos serviços que utilizam SSL
  - Trocar todas as senhas de serviços em servidores vulneráveis

- Promover ações que incentivem a troca periódica de senhas dos usuários da sua instituição .
  - Serviços internos (Intranet, E-mail, Wiki, VPN, etc.)
  - Serviços externos (e-mails, redes sociais, serviços em nuvem, etc)

http://www.rnp.br/cais/alertas/2014/openssl_1.html

RNP

Obrigado!

CAIS – Centro de Atendimento a Incidentes de Segurança

cais@cais.rnp.br