CERTISIGN
A sua identidade na rede

Comunicado

Ataque LogJam –
Nova vulnerabilidade no SSL/TLS

O que está acontecendo?

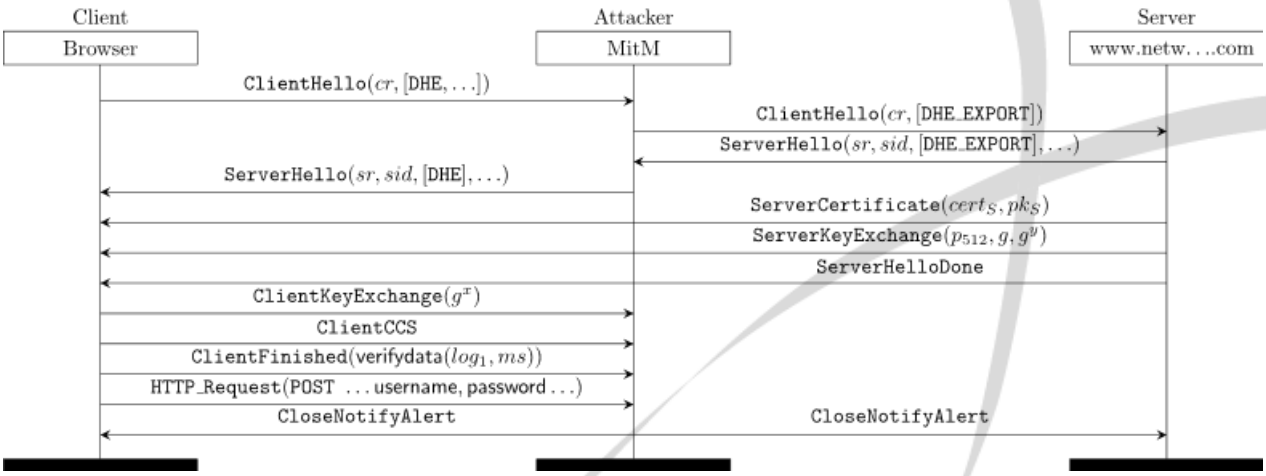
O setor de TI recentemente tem divulgando diversos ataques sobre os protocolos de criptografia. E na última semana, foi descoberta uma nova vulnerabilidade no protocolo TLS – protocolo que provê comunicação segura na internet. Esta vulnerabilidade é conhecida como **LOGJAM**, e aproveita uma falha no algoritmo "Diffie-Hellman Key Exchange" que possibilita a redução do nível de segurança de uma conexão.

Esta falha afeta qualquer servidor web com certificado digital SSL/TLS (HTTPS), assim como servidores de email (STMPS), servidores VPN (IPsec), navegadores (Browsers) ou qualquer outro servidor e software que suporte cifras "DHE_EXPORT".

Como funciona ?

O **LOGJAM** permite que um espião conhecido como man-in-the-middle (MITM) consiga realizar o downgrade de uma conexão segura, forçando que esta suporte a *ciphersuites* "DHE_EXPORT" que reduz a força da criptografia para 512bits – cifra relativamente fácil de ser quebrada.

Abaixo, ilustração de ataque feito pelo MITM:



Hoje, estima-se que o **LOGJAM** afeta em torno de 8,4% de um milhão dos sites mais visitados da internet, além de servidores de e-mail e outros serviços.

O que deve ser feito?

Os clientes deverão verificar a situação de seus ambientes e, em caso de detecção da vulnerabilidade apresentada, realizar os procedimentos abaixo:

- Servidores

É necessário desabilitar o suporte a "Export Cipher Suites" e gerar um único grupo DHE de 2048 bits.

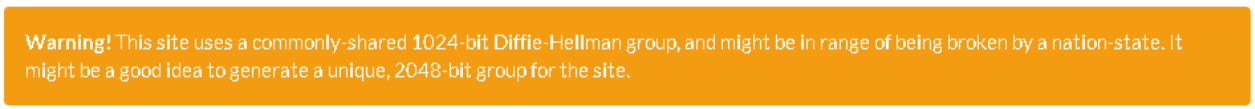
Como fazer isto? Existe um guia de instruções no link abaixo onde é possível verificar um "passo a passo" para corrigir esta falha em diversos servidores.

- https://weakdh.org/sysadmin.html

Já no link a seguir é possível verificar o status de seu servidor.

- https://weakdh.org/servercheck.html

Caso seja apresentada a mensagem de "Warning!", conforme imagem abaixo, o seu servidor está vulnerável ao ataque.



- SSH

É necessário atualizar tanto o ambiente servidor quanto o cliente para a versão mais recente do OpenSSH, que utiliza Elliptic Curve Diffie-Hellman-Key Exchange (ECDH).

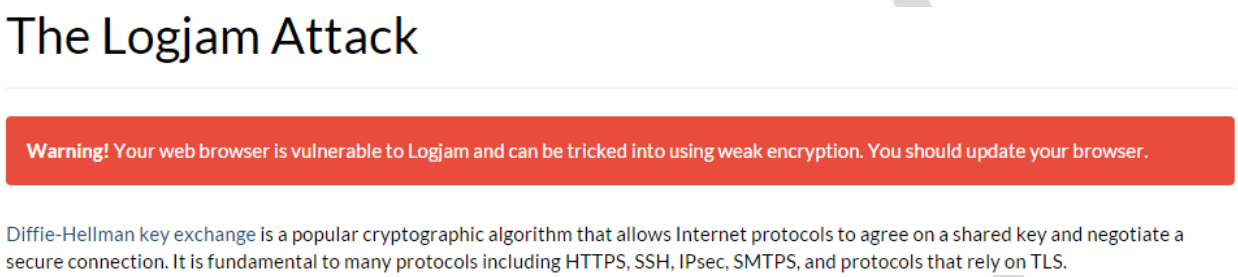
- **Navegadores**

Certifique-se de que você tem a versão mais recente do seu navegador instalado, e verifique se existem novas atualizações. Google Chrome (incluindo o navegador Android), Mozilla Firefox, Microsoft Internet Explorer, e Apple Safari estão realizando correções e lançando novas atualizações para corrigir este ataque.

No link disponibilizado abaixo é possível verificar o status de seu navegador:

- https://weakdh.org/

Caso seja apresentada a mensagem de "Warning!", conforme imagem abaixo, o seu navegador está vulnerável ao ataque.



Perguntas frequentes

1. Preciso substituir meu certificado digital SSL em caso de vulnerabilidade?

R: Não é necessário substituir seu certificado digital SSL, apenas realizar as correções apresentadas acima.

P: Meus serviços hospedados na Certisign estão seguros?

R: Sim.

3. Se não corrigir esta falha, o que pode acontecer?

R: Caso seu servidor esteja vulnerável a esta nova falha, potencialmente você estará vulnerável a ataques que permitem o roubo de informações protegidas pelo seu SSL.

Referências.

https://weakdh.org/

https://weakdh.org/imperfect-forward-secrecy.pdf

http://labs.siteblindado.com/2015/05/logjam-nova-falha-que-afeta-o-ssl.html

http://www.theregister.co.uk/2015/05/20/logjam_johns_hopkins_cryptoboffin_ids_next_branded_bug

Atenciosamente,

pos_venda@certisign.com.br

11 4501-1867 / 1962