CAIS-Alerta: Vulnerabilidade no OpenSSL - Atualização 1

[RNP, 24.04.2014, revisão 01]

O CAIS publicou no dia 10 de abril de 2014 um alerta sobre a vulnerabilidade na biblioteca OpenSSL, amplamente utilizada para prover comunicação segura e privacidade na internet, para diversos serviços e aplicativos.

Essa vulnerabilidade permite roubar informações protegidas, logo, sua exploração poderá expor senhas ou outras informações sensíveis. Diante disso, o CAIS lança uma atualização do alerta Vulnerabilidade no OpenSSL.

Nessa atualização, salienta-se a importância da substituição dos certificados digitais e das senhas nos sistemas e serviços afetados pela falha, bem como a geração de novas chaves secretas.

Impacto

Ainda que as recomendações do alerta anterior já tenham sido aplicadas, as informações sensíveis, como senhas, chaves secretas e certificados digitais, podem ter sido comprometidas. Da mesma forma, um atacante pode espionar as comunicações, roubar dados dos sistemas e serviços entre outras atividades ilícitas.

O CAIS já registrou tentativas de exploração dessa vulnerabilidade.

Recomendações

- Verificar e executar as recomendações do alerta Vulnerabilidade no OpenSSL, caso ainda não tenham sido aplicadas. A saber:
- Executar o comando abaixo em um sistema UNIX-LIKE ou Windows e verifique a versão instalada: #openssl version -a
- OBS: Para sistemas Windows, o comando acima deve conter também o diretório de instalação do OpenSSL.
- Ferramenta online para realizar o teste https://www.ssllabs.com/ssltest/index.html
- Ferramenta NMAP: https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse
- Corrigir a vulnerabilidade identificada:
-

  Atualize o OpenSSL para a versão 1.0.1g ou a mais recente recomendada pelos desenvolvedores.

- Desabilitar o suporte ao OpenSSL Heartbeat
-

Esse problema pode ser tratado recompilando o OpenSSL com a flag -DOPENSSL_NO_HEARTBEATS.

Aplicativos que utilizam o OpenSSL, como o Apache ou Nginx, deverão ser reiniciados para que as mudanças sejam efetivadas.

- Utilize Perfect Forward Secrecy (PFS)
-

PFS pode ajudar a minimizar os danos em caso de vazamento de uma chave secreta fazendo com que seja mais difícil decifrar o tráfego de rede já capturado.

- Implementar assinaturas no IDS
-

Visando mitigar qualquer risco associado a um possível comprometimento de senhas, chaves secretas ou certificados, o CAIS recomenda adicionalmente:

- Trocar certificados de serviços que utilizem SSL, como imaps, smtps, ftps, pops, (Open)VPN, https;

- Trocar senhas de serviços hospedados em servidores considerados vulneráveis;

- Promover ações que incentivem os usuários da sua instituição a realizarem a troca de senhas associados a sistemas e serviços corporativos (Intranet, wiki, VPN entre outros)

- Promover ações de conscientização entre os usuários da sua instituição para troca de senhas de serviços externos (Gmail, Yahoo mail, Hotmail/Outlook entre outros). Veja tabela abaixo:

http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

Informamos também que já existem atualizações para correção das vulnerabilidades em VMware. As versões afetadas, assim como as atualizações, encontram-se em http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Mais informações

- https://isc.sans.edu/forums/diary/+Patch+Now+OpenSSL+Heartbleed+Vulnerability/17921http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/
- http://www.openssl.org/news/secadv_20140407.txt
- http://arstechnica.com/security/2014/04/confirmed-nasty-heartbleed-bug-exposes-openvpn-private-keys-too/
- http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Identificador CVE (http://cve.mitre.org):
CVE-2014-0160

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os Alertas do CAIS também são oferecidos no formato RSS/RDF e no Twitter:
http://www.rnp.br/cais/alertas/rss.xml
Siga @caisrnp.