CAIS-Alerta: Vulnerabilidade no OpenSSL

[RNP, 10.04.2014, revisão 01]

O CAIS alerta sobre a recente vulnerabilidade presente na biblioteca OpenSSL, que é utilizada nos protocolos SSL, TLS e DTLS. A biblioteca OpenSSL é utilizada para prover comunicação segura e privacidade na internet para diversos serviços e aplicativos, tais como: sistemas de email, navegadores web, mensagens instantâneas(IM), VPNs, entre outros.

Impacto

Um usuário mal intencionado, através de pacotes manipulados, pode ser capaz de recuperar as chaves secretas utilizadas nos sistemas para cifrar informações sensíveis. Dessa forma, um atacante pode espionar as comunicações, roubar dados diretamente dos sistemas/serviços e enganar os usuários se fazendo passar por um fornecedor de serviços.

Até a divulgação deste alerta, existem relatos de exploração da vulnerabilidade no OpenSSL.

Recomendações

- Verificar se o sistema está vulnerável
-

  Até a divulgação desse alerta, existem relatos de exploração da vulnerabilidade no OpenSSL.

  Execute 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
-

Este 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
-

http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/

Versões afetadas

- OpenSSL 1.0.1f
- OpenSSL 1.0.1e
- OpenSSL 1.0.1d
- OpenSSL 1.0.1c
- OpenSSL 1.0.1b
- OpenSSL 1.0.1a
- OpenSSL 1.0.1

Mais informações

- https://isc.sans.edu/forums/diary/+Patch+Now+OpenSSL+Heartbleed+Vulnerability/17921
- http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/
- http://www.openssl.org/news/vulnerabilities.html
- http://heartbleed.com/
- http://www.openssl.org/news/secadv_20140407.txt
- http://exame.abril.com.br/tecnologia/noticias/falha-grave-no-openssl-deixa-dados-sigilosos-vulneraveis?page=2

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.