CAIS-Alerta: Vulnerabilidade possibilita ataque Man-in-the-Middle envolvendo o OpenSSL

[RNP, 13.06.2014-, 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 poderia enviar uma mensagem maliciosa (ChangeCipherSpec message) durante o handshake do TLS, precisamente antes da chave de sessão ser gerada, dessa forma, ele poderia realizar um ataque do tipo main-in-the-middle, obtendo assim informações trocadas entre cliente e servidor.

É importante salientar que a realização desse ataque depende das seguintes condições serem satisfeitas:

Primeiro: O usuário malicioso precisa estar na mesma rede que as vítimas (cliente e servidor).

Segundo: O usuário malicioso precisa forçar a utilização de chaves de criptografia frágeis, visto que ele precisa descobrir o hash gerado na comunicação entre cliente e servidor durante o handshake.

Vale lembrar quer os principais browsers (Internet Explorer, Firefox, Chrome e Safari) não são vulneráveis ao ataque contra o OpenSSL.

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

Recomendações

- Verificar se o sistema está vulnerável
-

  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.

- Corrigir a vulnerabilidade identificada
-

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

- Todos os aplicativos que utilizam o OpenSSL deverão ser reiniciados para que as mudanças sejam efetivadas.
-

Versões afetadas

- OpenSSL 1.0.1 - Versão server
- OpenSSL 1.0.2-beta1 - Versão server

Mais informações

- 1 - Análise da vulnerabilidade no OpenSSL
- 2 - Latest OpenSSL bug ‘may be more dangerous than Heartbleed’
- 3 - OpenSSL Security Advisory

Identificador CVE (http://cve.mitre.org):
CVE-2014-0224

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.