Alerta de Segurança 002/2014 - CGTI/VPGDI

Em 9 de abril de 2014

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidade no OpenSSL "The Heartbleed Bug"

Prezados Gestores,

Encaminhamos, na íntegra, o alerta emitido pela Coordenação-Geral de Tratamento e Incidentes de Redes / Departamento de Segurança da Informação e Comunicações sobre vulnerabilidade no OpenSSL.

1. Descrição do Problema

"The Heartbleed Bug" é uma vulnerabilidade grave encontrada no OpenSSL. A vulnerabilidade permite acesso às informações criptografadas por SSL / TLS usadas na Internet em aplicações Web, e-mail e em algumas redes privadas virtuais (VPNs).

Versões do OpenSSL vulneráveis:

- OpenSSL 1.0.1 até 1.0.1f (inclusive)
- OpenSSL 1.02-beta.

Sistemas Operacionais com OpenSSl possivelmente comprometidos:

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4.
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11.
- CentOS 6.5, OpenSSL 1.0.1e-15.
- Fedora 18, OpenSSL 1.0.1e-4.
- OpenBSD 5.3 OpenSSL 1.0.1c (10 de maio de 2012) e 5.4 OpenSSL 1.0.1c (10 de maio de 2012).

- FreeBSD 10.0 - OpenSSL 1.0.1e (11 de fevereiro de 2013).
- NetBSD 5.0.2 (OpenSSL 1.0.1e).
- OpenSUSE 12.2 (OpenSSL 1.0.1c).

2. Possíveis Riscos

- Quebra da privacidade e segurança das informações criptografadas trafegadas em rede.
- Possibilita ao atacante comprometer as chaves secretas.

3. Sugestões para Mitigação do Problema

- Instalar a versão mais atual do OpenSSL – (OpenSSL 1.0.1g).
- Efetuar a revogação das chaves, que possivelmente estão comprometidas, e fazer a reemissão e distribuição de novas chaves.

Mais informações podem ser encontradas em:

- https://www.openssl.org/news/secadv_20140407.txt
- http://heartbleed.com
- https://isc.sans.edu/forums/diary/OpenSSL+CVE-2014-0160+Fixed/17917
- http://sseguranca.blogspot.com.br/2014/04/heartbleed-ssl-bug.html
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- http://s3.jspenguin.org/ssltest.py
- http://www.exploit-db.com/exploits/32745/

Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações