Alerta de Segurança 002/2016 - CGTI/VPGDI

Em 20 de maio de 2016

Para: Gestores de TI das unidades da Fiocruz
Assunto: Vulnerabilidade do Protocolo SSL 3.0

1. Descrição do problema

Uma vulnerabilidade no protocolo SLLv3 permite um ataque que tem como alvo as cifras de modo CBC. A vulnerabilidade permite um ataque MITM (*man-in-the-middle*), onde um usuário malicioso consegue interceptar conexões 'seguras' entre um cliente e um servidor. Tal falha no protocolo é conhecida como "Poodle" (*Padding Oracle On Downgraded Legacy Encryption*).

Seguem sugestões passadas pelo CAIS (Centro de Atendimento a Incidente de Segurança) para auxílio na identificação da vulnerabilidade.

```
1 - Teste usando openssl
$openssl s_client -ssl3 -connect "IP ou domínio":443


Caso apareça na saída do comando a linha abaixo você está vulnerável
"SSL handshake has read 7 bytes and written 0 bytes"
"---"
"New, (NONE), Cipher is (NONE)"
"Secure Renegotiation IS NOT supported"


2 - Teste usando cURL
$curl -v3 -X HEAD https://"IP" ou "dominio"


Caso apareça na saída do comando algo parecido com a linha abaixo você não está
vulnerável
"SSL peer handshake failed"
```

2. Sugestão para mitigação

Para correção, de uma forma geral, recomenda-se usar as funções do seu servidor WEB que suportam TLS_FALLBACK_SCSV, impedindo que invasores forcem os navegadores a utilizar SSL 3.0, ou ainda desativar o protocolo SSL 3.0 ou SSL 3.0 *cipher CBC-mode*.

No entanto, ressalta-se que antes de desativar um serviço e/ou atualizá-lo, o mesmo deve ser testado em ambientes de homologação, evitando assim uma eventual parada de um serviço em ambiente de produção.

3. Informações complementares

Informações adicionais podem ser obtidas nos links abaixo:

https://www.us-cert.gov/ncas/alerts/TA14-290A

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://poodle.io/

Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações