Alerta de Segurança 003/2016 - CGTI/VPGDI

Em 23 de maio de 2016

Para: Gestores de TI das unidades da Fiocruz
Assunto: Drown Attack

1. Descrição do problema

Recentemente foi descoberto um ataque chamado *Drown Attack,* que consiste em explorar vulnerabilidades nas aplicações e serviços que utilizam o protocolo SSL/TLS, como por exemplo o HTTPS. O ataque tem potencial para comprometer a confidencialidade e a integridade das informações criptografadas trocadas entre o cliente e o servidor.

2. Sugestão para mitigação

Para mitigar o problema, recomenda-se atualizar o OpenSSL para as versões 1.0.1s ou 1.0.2g e desativar o protocolo SSLv2 de serviços como: WEB, SMTP, IMAP, POP, entre outros.

3. Informações complementares

Para identificar se o serviço está vulnerável, utilize a ferramenta disponível no endereço https://test.drownattack.com

Informações técnicas detalhadas estão disponíveis no artigo https://drownattack.com/drown-attack-paper.pdf

Atenciosamente,

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