CORREGEDORIA-GERAL DA JUSTIÇA DO ESTADO DE SANTA CATARINA
NÚCLEO IV - SERVENTIAS EXTRAJUDICIAIS

COMUNICADO n. 01/2017

Adequação dos sistemas da serventia aos serviços do Selo Digital de Fiscalização face à atualização de segurança de componente em seus servidores

Prezados Srs. Notários e Registradores,

A Comissão dos Sistemas Eletrônicos Extrajudiciais comunica que os senhores delegatários deverão entrar em contato com os responsáveis pelos sistemas de automação da serventia para que adotem as providências necessárias a fim de mitigar riscos à segurança, conforme descrição técnica detalhada abaixo por nossa equipe de tecnologia, **até o prazo de 15/05/2017**.

ATUALIZAÇÃO DE SERVIDORES APACHE COM SSL – DESCRIÇÃO TÉCNICA

No intuito de mitigar o risco de segurança decorrente da vulnerabilidade "CVE-2016-2017" apelidada de "Padding Oracle Vulnerability", em que um ataque do tipo "man in the middle" pode se aproveitar dela para descriptografar os dados trafegados em determinados algoritmos de criptografia, será necessário atualizar alguns componentes da infraestrutura que suporta o serviço do Selo Digital.

Para tanto, uma atualização do componente **OpenSSL** que opera no canal de comunicação https://app.tjsc.jus.br/selo20/SeloService será necessária. Essa atualização pode causar falha na comunicação com o webservice em alguns casos, mais notadamente em versões mais antigas de alguns sistemas operacionais que suportam os sistemas clientes do webservice.

Um ambiente de homologação específico para testar a atualização do componente foi disponibilizado. Os stubs podem ser gerados a partir da URL http://selo.tjsc.jus.br/SeloServiceTesteSSL?wsdl O endpoint do serviço passa a ser **https://selo-hml.tjsc.jus.br/selo_teste/SeloService**

Neste contexto, pedimos que as empresas fornecedoras de softwares para as serventias verifiquem a compatibilidade de seus sistemas com o ambiente acima, e promovam os ajustes necessários para que a **atualização** do ambiente de **produção** previsto para **15/05/2017** não cause problemas ou interrupção nos sistemas clientes que afetem os envios de atos ou recebimento de selos.

O exíguo prazo deriva da necessidade de manter o ambiente seguro e confiável e por este motivo o esforço para os testes e adequações se justificam diante da necessidade.

Maiores informações a respeito da vulnerabilidade podem ser obtidas nos links abaixo:
https://blog.cloudflare.com/yet-another-padding-oracle-in-openssl-cbc-ciphersuites/
https://www.openssl.org/news/vulnerabilities.html

Pretende-se com o presente, reforçar a necessidade de que Vossas Senhorias possam acompanhar e diligenciar junto aos Vossos fornecedores para que adotem, no prazo fixado, todas as providências recomendadas.

Eventuais dúvidas poderão, como de costume, ser encaminhadas para selodigital@tjsc.jus.br.

Florianópolis, 20 de abril de 2017.

Atenciosamente,
Comissão de Sistemas Eletrônicos Extrajudiciais
Núcleo IV – Serventias Extrajudiciais
Corregedoria-Geral da Justiça de Santa Catarina