Prezados,

O CAIS alerta para a publicação de três correções de segurança para a 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.

Descrição

ChaCha20/Poly1305 heap-buffer-overflow (CVE-2016-7054) - Severidade: Alta
==========
Conexões TLS utilizado cifras *-CHACHA20-POLY1305 estão suscetíveis a ataques de negação de serviço, através do envio de uma grande quantidade de dados corrompida; não há registro de que a exploração desta vulnerabilidade possa causa algum dano além de indisponibilidade de serviço.

CMS Null dereference (CVE-2016-7053) - Severidade: Moderada
==========

Aplicações processando estruturas CMS inválidas podem gerar erro "NULL pointer dereference", causado por um bug no tratamento do tipo ASN.1 CHOICE.

Multiplicação Montgomery pode produzir resultados incorretos (CVE-2016-7055) - Severidade: Baixa
==========

Um bug no procedimento de multiplicação Montgomery, que manipula entradas divisíveis por e maiores que 256 bits, pode apresentar resultados incorretos. Neste caso, poderiam ocorrer falhas em autenticação e negociação de chaves.

Sistemas impactados

Sistemas utilizando a biblioteca OpenSSL em versões 1.1.0 anteriores a 1.1.0c

Versões afetadas

Versões anteriores a 1.1.0c

Correções disponíveis

Atualizar a versão do OpenSSL para a versão mais recente

disponibilizada pelos desenvolvedores (1.1.0c no momento da publicação deste alerta) ou a versão mais recente recomendada de acordo com o sistema operacional em uso. É recomendada a reinicialização dos serviços que utilizem esta biblioteca após a atualização.

Identificadores CVE (http://cve.mitre.org)
CVE-2016-7054
CVE-2016-7053
CVE-2016-7055

Mais informações
https://www.openssl.org/news/secadv/20161110.txt

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 Twitter: Siga @caisrnp

Atenciosamente,
CAIS/RNP