CAIS-Alerta [16/10/2017]: Vulnerabilidade no protocolo de redes sem-fio "Wi-fi Protected Access II" (WPA2)

Prezados,

O CAIS alerta para vulnerabilidade recente envolvendo o protocolo de redes sem-fio "Wi-fi Protected Access II" (WPA2). Até o momento da divulgação deste alerta haviam sido públicadas provas de conceito (PoC) referentes ao ataque juntamente com o artigo disponibilizado pelos pesquisadores responsáveis pela descoberta.

Descrição

Durante a fase de acesso de um cliente em uma rede WPA2, existe um processo de negociação de parâmetros de comunicação entre cliente e servidor (Access Point - AP) onde tais parâmetros podem ser manipulados. Dessa forma, por exemplo, chaves de criptografia utilizadas para cifragem de dados transmitidos podem ser reinstaladas pelo cliente ou AP.

Um atacante, dentro da área de alcance do AP, pode posicionar-se entre cliente e AP sendo capaz de coletar informações sensíveis ou mesmo injetar dados de forma arbitrária na sessão em questão. As formas de manipulação de dados podem variar de acordo com os protocolos de confidencialidade de dados utilizados (ex.: TKIP, GCMP ou AES-CCMP).

Sistemas impactados

Sistemas de redes sem-fio que utilizem o protocolo WPA2.

Versões afetadas

A vulnerabilidade existe na implementação do protocolo WPA2, sendo assim é independente de versão.

Correções disponíveis

Os diversos desenvolvedores de software e hardware que utilizam o protocolo WPA2 estão disponibilizando atualizações que corrigem a forma como seus sistemas interagem com a implementação do protocolo WPA2. Sendo assim, recomenda-se que sejam seguidas as orientações dos desenvolvedores ou fabricantes para mitigação da vulnerabilidade.

Identificadores CVE (http://cve.mitre.org)
CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081,
CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088.

Mais informações
https://www.krackattacks.com/
http://www.kb.cert.org/vuls/id/228519
https://papers.mathyvanhoef.com/ccs2017.pdf

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 podem ser acompanahadas pelas redes sociais da RNP. Siga-nos!!

Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

Atenciosamente,

CAIS/RNP


```
#####################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)          #
#       Rede Nacional de Ensino e Pesquisa (RNP)                    #
#                                                                   #
# cais em cais.rnp.br    http://www.rnp.br/servicos/seguranca       #
# Tel. 019-37873300      Fax. 019-37873301                          #
# Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key       #
#####################################################################
```