Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 06/2017 – Vulnerabilidade *WPA2 KRACK*

1. Descrição do Problema

Foi encontrada uma vulnerabilidade no protocolo WPA2. Esta vulnerabilidade foi descoberta pelos pesquisadores Mathy Vanhoef of imec-DistriNet, da Universidade Católica de Leuven, Belgica.

Quando um cliente se conecta a uma rede WI-FI um aperto de mão (handshake) é feito para verificar se o dispositivo tem a senha correta. Além disso, o cliente recebe uma chave criptográfica que é utilizada para proteger qualquer dado subsequente. A falha permite que o atacante resete essa chave e, com isso, descriptografe todo o tráfego da vítima.

2. Métodos de Ataques

Quando um cliente se conecta a uma rede, ele executa a negociação chamada 4-way handshake para negociar uma nova chave de sessão. Ele instala essa chave após receber a mensagem 3 do handshake. Uma vez que a chave esteja instalada, ela será usada para criptografar quadros de dados usando um protocolo de confidencialidade. No entanto, como as mensagens podem ser perdidas ou descartadas, o ponto de acesso (AP) retransmitirá a mensagem 3 se não receber uma resposta adequada como confirmação. Como resultado, o cliente pode receber a mensagem 3 várias vezes. Cada vez que recebe esta mensagem, ela reinstalará a mesma chave de sessão e recebe o número de pacote de transmissão incremental (nonce) e recebe o contador de repetição usado pelo protocolo de confidencialidade de dados.

Para a realização do ataque, ou seja, para forçar o reenvio da mensagem 3 do 4-way handshake, um atacante precisa realizar um ataque de man-in-the-minddle (MitM) de forma a se posicionar entre o cliente e o AP. A partir de então, os pacotes podem ser repetidos, descriptografados e / ou forjados. A mesma técnica também pode ser usada para atacar a chave de grupo, PeerKey, TDLS e BSS.

3. Sistemas afetados

As implementações do iOS (Apple) e da Microsoft, não permitem a retransmissão da mensagem 3, o que vai contra a especificação do protocolo mas acaba livrando os dispositivos destes fabricantes de parte das vulnerabilidades encontradas. Já a implementação do Linux e do Android 6.0 ou superior é bastante afetada.

4. Sugestões para Mitigação do Problema

- mantenha os sistemas atualizados para a versão mais recente ou aplique os patch conforme orientação do fabricante. As principais empresas de sistemas operacionais, smartphones, roteadores já estão desenvolvendo patch para correção da falha;
- efetue autenticação em conexões seguras (HTTPS, por exemplo);
- utilize uma VPN;
- considere estabelecer o modo “Rede Pública” em conexões wi-fi;
- Por fim, realize campanhas internas, alertando os usuários sobre esta publicação.

5. Referências

- http://dsic.planalto.gov.br/legislacao/RequisitosMnimosSIparaAPF.pdf/view
- https://www.kb.cert.org/vuls/id/228519/
- https://cwe.mitre.org/data/definitions/323.html
- https://papers.mathyvanhoef.com/ccs2017.pdf
- https://www.krackattacks.com/
- https://morphuslabs.com/sobre-o-wpa2-krack-attack-b999efccb106
- https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/80211i/funcionamento.html

Brasília-DF, 16 de outubro de 2017.

Equipe do CTIR Gov