Kr00k

Amarildo Felix Ribeiro Junior[1]
Anderson santos da silva [2]
Jader Ligório Rodrigues [3]

RESUMO

Kr00k é uma vulnerabilidade em detectada em chips wi-fi fabricados pela Broadcom e pela Cypress. Pesquisadores da ESET descobriram uma brecha estrutural que afeta a criptografia de redes WLAN. Essa vulnerabilidade permite que um atacante visualize os pacotes de dados transmitidos através de uma rede local sem fio que seja protegida com WPA2 CCMP sofram com o problema.

Palavras-chave: Redes, wi-fi, vulnerabilidade, kr00k.

ABSTRACT

Kr00k is a vulnerability in detected on wi-fi chips manufactured by Broadcom and Cypress. ESET researchers have discovered a structural loophole that affects the encryption of WLAN networks. This vulnerability allows an attacker to view data packets transmitted over a wireless LAN that is protected with WPA2 CCMP and suffer from the problem.

Keywords: Networks, wi-fi, vulnerability, kr00k.

[1] Acadêmica do Curso Superior em Tecnólogo em Redes de Computadores – Faculdade Alcides Maya. amarildo.junior@alcidesmaya.edu.br

[2] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br

[3] Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. jader_rodrigues@alcidesmaya.edu.br

Como resumidamente dito, trata-se de uma vulnerabilidade de rede WLAN, podendo ser considerada extremamente grave e preocupante. O atacante não precisa nem mesmo saber a senha da rede para cometer uma invasão, o que acelera o possível ataque e também facilita o mesmo.

Tratando-se de falha estrutural em chips de grandes fabricantes a nível mundial de distribuição, fica fácil de imaginar a grande abrangência desse risco para incontáveis usuários, que em grande parte utilizam protocolo WPA2 CCMP em suas redes. Imagine ainda grandes fabricantes como Apple, Nexus, Samsung, entre outros, com milhões de equipamentos expostos a esta falha.

Esta vulnerabilidade foi apresentada em fevereiro de 2020, nos Estados Unidos, durante a RSA Conference 2020. de forma resumida, o problema está no fato de que os dispositivos vulneráveis usam uma chave de criptografia composta inteiramente por zeros para proteger parte da comunicação sem fio. Dessa forma, qualquer criminoso com o mínimo de conhecimento em redes consegue descriptografar os pacotes (que não estejam na camada TLS; ou seja, sites que usam HTTPS estão seguros) para espionar o que você está acessando.

A forma de evitar esta vulnerabilidade é mantendo os equipamentos sempre atualizados. Alguns fabricantes como Cisco e Hauwey mencionaram intenção de lançarem atualizações para correção desta falha na ocasião em que foi apresentado a falha, mas nem todos os fabricantes tem a devida preocupação e/ou intenção de lançar tal correção (por mais que possa ser uma minoria.

Grande parte dos usuários acreditam as vezes que atualizações não são tão necessárias, esta vulnerabilidade evidencia a importância de dar a devida atenção para este ponto. Muitas atualizações corrigem brechas como essa, entre outras, além de impactar no desempenho dos aparelhos.

Outra coisa que pode ser relevante, utilizar protocolos alternativos na rede WLAN, como por exemplo, WEP o WPA-TKIP e o novo WPA3. Grande maioria dos usuários sempre mantém padrões simples, muitas vezes por desconhecimento. Boa parte dos técnicos também não tem esse conhecimento, nem chegam a oferecer opções alternativas para seus clientes. Fica a

reflexão sobre buscar alternativas diferentes e sair da zona de conforto, e do comum, enquanto profissionais de TI, principalmente em redes.

REFERÊNCIAS

https://thehack.com.br/conheca-a-kr00k-nova-vulnerabilidade-que-assola-bilhoes-de-dispositivos-wifi/

https://www.eset.com/int/kr00k/

https://www.hackread.com/billions-of-wi-fi-devices-affected-by-kr00k-encryption-vulnerability/

https://www.zdnet.com/article/cisco-says-patches-incoming-to-address-new-kr00k-vulnerability-impacting-routers-firewall-products/

https://www.huawei.com/en/psirt/security-notices/huawei-sn-20200228-01-kr00k-en