BOLETÍN DE ALERTA

Boletín Nro.: 2020-06

Fecha de publicación: 02/03/2020

Tema: Vulnerabilidad en chips WiFi fabricados por Broadcom y Cypress permiten descifrar el tráfico de la red y acceder a los paquetes contenidos en él.

CVE-2019-15126

Sistemas afectados:

Dispositivos que utilizan chips WiFi fabricados por Broadcom y Cypress (Teléfonos inteligentes, tabletas, ordenadores, router, dispositivos IoT).

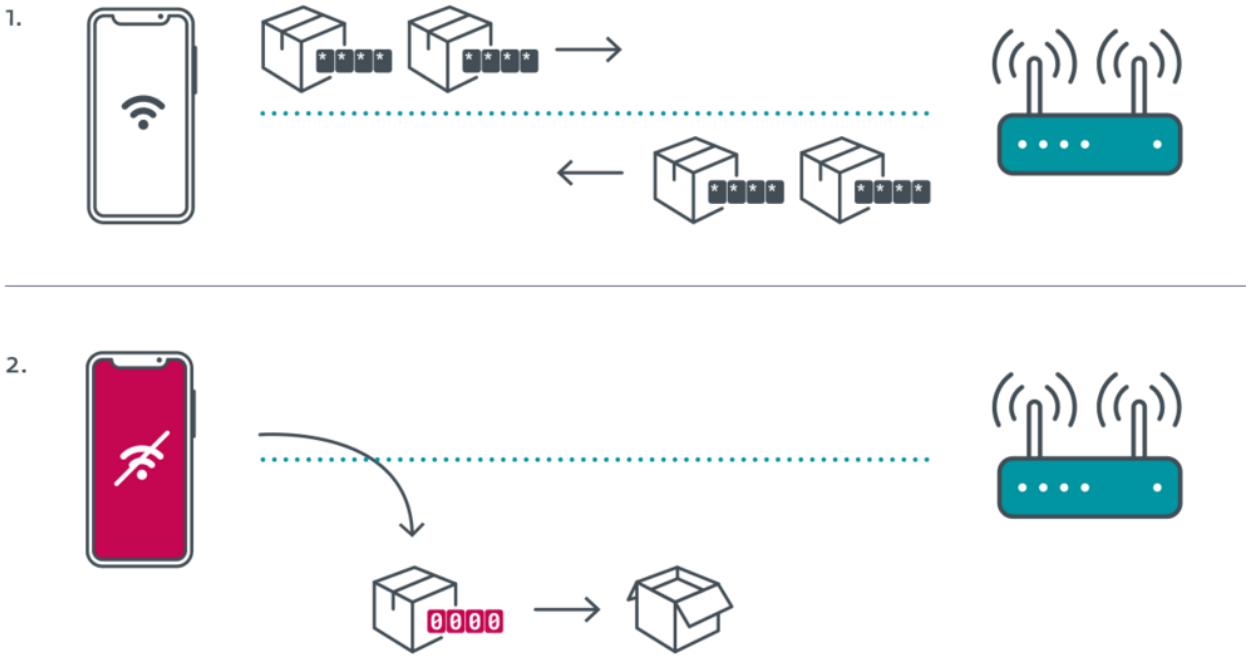
Descripción:

Recientemente un grupo investigadores ha descubierto una vulnerabilidad bautizada como **Kr00k** en los chips WiFi de los fabricantes **Broadcom** y **Cypress**, la misma permite a un atacante descifrar el tráfico de la red y acceder a los paquetes contenidos en él.

El atacante no necesita estar conectado a la red inalámbrica de la víctima, la falla funciona únicamente contra los dispositivos vulnerables que usan protocolos WPA2-Personal o WPA2-Enterprise, con encriptación AES-CCMP, para proteger el tráfico de la red.

Los paquetes enviados durante la comunicación son cifrados con una clave única que depende de la contraseña establecida por el usuario, la falla se da cuando el usuario se desconecta repentinamente de la red inalámbrica, esta desconexión ocurre habitualmente cuando hay una señal de WiFi baja o algún problema, a la misma se la denomina **"desconexión temporal"**. Lo habitual en una desconexión temporal es que los chips WiFi se configuren automáticamente para volver a conectarse a la red, sin perder su valor de cifrado, pero en este caso los chips WiFi vulnerables establecen el

valor de cifrado a 0.



Por lo tanto, un atacante puede forzar a que los dispositivos se desconecten de la red enviando paquetes de desautenticación y luego usar el **Kr00k** para descifrar el tráfico de la red usando el valor de cifrado 0.

1	0.000000	52.114.158.53	192.168.100.3	TLSv1.2	442 Application Data
2	0.000001			ICMPv6	122 Neighbor Advertisement rtr, sol, ovr) is at
4	0.000003	74.125.133.188	192.168.100.3	TLSv1.2	202 Application Data
6	0.000005	192.168.100.31	192.168.100.1	ICMP	426 Echo (ping) request id=0x002a, seq=0/0, ttl=64 (no response found!)
7	0.000006	[redacted]	192.168.100.2	TCP	106 443 → 60189 [ACK] Seq=1 Ack=1 Win=257 Len=0 TSval=2807327454 TSecr=119601448
14	0.000013	[redacted]	192.168.100.2	TLSv1.2	554 Application Data
19	0.000018	[redacted]	192.168.100.2	TLSv1.2	474 Application Data
26	0.000025	[redacted]	192.168.100.2	TLSv1.2	138 Application Data
33	0.000032	[redacted]	192.168.100.2	TLSv1.2	122 Application Data
40	0.000039	172.217.23.225	192.168.100.2	TCP	106 443 → 60035 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=527934487 TSecr=119654013 WS=256
46	0.000045	SamsungE_	Broadcast	ARP	74 Who has 192.168.1.1? Tell 192.168.1.28
47	0.000046	192.168.100.153	172.217.23.202	TCP	106 49491 → 443 [FIN, ACK] Seq=1 Ack=1 Win=819 Len=0 TSval=738690 TSecr=532191579
48	0.000047	Apple_		EAPOL	58 Logoff
49	0.000048	Apple_	AsustekC_	ARP	74 Who has 192.168.1.1? Tell 192.168.1.249

Ejemplo de tráfico WLAN capturado.

Cabe destacar que, aunque su dispositivo sea vulnerable, no significa que la contraseña del Wi-Fi se haya visto comprometida.

Impacto:

Un atacante que logre la desconexión de los dispositivos vulnerables de la red WiFi, mediante el envío de paquetes de desautenticación, podría capturar los paquetes descifrados de la red, incluyendo los paquetes DNS, ARP, ICMP, HTTP, TCP y TLS. Esta vulnerabilidad no afecta a los paquetes que viajan por medio del protocolo HTTPs.

Solución y Prevención

Aplicar los parches de seguridad correspondiente a cada dispositivo vulnerable. Para ello debe verificar si el fabricante de su dispositivo ha lanzado una actualización de seguridad y aplicarla lo más pronto posible.

Los parches conocidos hasta la fecha que abordan esta vulnerabilidad, son:

- macOS Catalina 10.15.1, Actualización de seguridad 2019-001 y Actualización de seguridad 2019-006 - 29 de octubre de 2019
- Actualización de seguridad para iOS 13.2 y iPadOS 13.2 - 28 de octubre de 2019
- Aviso de seguridad de Cisco 20200226 - 27 de febrero de 2020
- Aviso de seguridad de Huawei 20200228-01 - 28 de febrero de 2020

Información adicional:

- https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf
- https://www.hackread.com/billions-of-wi-fi-devices-affected-by-kr00k-encryption-vulnerability/
- https://thehackernews.com/2020/02/kr00k-wifi-encryption-flaw.html