ALERTA DE SEGURIDAD

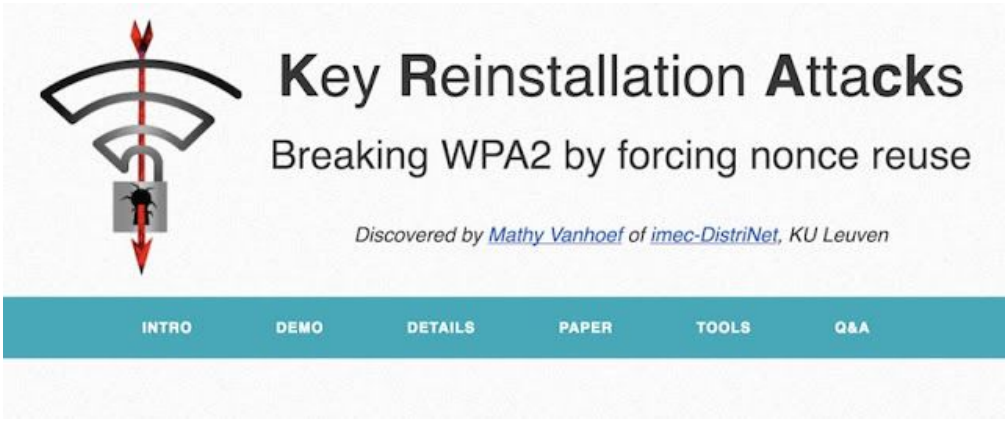
Contenido

NIVEL DE ALERTA

Crítica

DESCRIPCIÓN DE LA AMENAZA

El **Centro de Seguridad y Vigilancia Digital** de A3SEC ha sido alertado sobre nuevas vulnerabilidades en el protocolo WI-FI Protected Access II (WPA2). Esta es la primera vulnerabilidad que se ha encontrado en este protocolo, ya que hasta el momento solo existían Ataques de fuerza bruta a las claves de cifrado WPA2-PSK.



Explotar esta vulnerabilidad podría permitir a un atacante dentro de la rango de la WIFI, interceptar cierto tipo de comunicaciones. Además, afecta a todas y cada una de las redes WiFi actuales protegidas y a todos los dispositivos que utilicen dicho protocolo (WPA2).
Esta vulnerabilidad ha sido encontrada recientemente por el investigador Mathy Vanhoef, de la universidad belga KU Leuven, que ha bautizado como KRACK, Key Reinstallation

Attacks. Afecta en una u otra manera a cualquier plataforma como Android, Linux, Windows, OpenBSD, MediaTek, Linksys, etc

El eje principal vector del ataque se centra en el four-way handshake del protocolo WPA2. Este procedimiento (handshake) se utiliza para comprobar las credenciales cuando un usuario está intentando unirse a una red WiFi. Durante este proceso se generan claves nuevas de cifrado, las cuales se instalan después de recibir el Mensaje 3 de los 4 y que sirven para proteger la sesión del usuario que está intentando conectarse a la WiFi.

La vulnerabilidad que explota KRACK permite al atacante manipular o repetir de nuevo este tercer Mensaje, permitiendo reinstalar la clave criptográfica que ya se ha utilizado. Y esto es importante para poder salvaguardar la seguridad del protocolo WPA2 ya que una clave criptográfica sólo puede ser utilizada una vez durante este proceso.

Este es un resumen simplificado del proceso que realiza KRACK:

1. El atacante intenta unirse a una red WiFi.
2. Comienza el proceso four-way handshake.
3. Se negocia una nueva clave de cifrado en el Mensaje 3 del proceso.
4. No se envía la señal de acknowledgment (reconocimiento) que verifica que se ha recibido el Mensaje 3 correctamente.
5. Esto fuerza que el punto de acceso (AP) retrasmita de nuevo el Mensaje 3 varias veces.
6. Este proceso repetido varias veces, siempre instalará la misma clave de cifrado y por lo tanto reseteará a cero nonce (número aleatorio el cual precisamente se encarga de evitar que se pueda repetir ataques y que actúa como contador de los paquetes transmitidos.
7. El atacante puede en este punto forzar estos reseteos nonce recolectándolos y repitiendo retrasmisiones del Mensaje 3.
8. Reutilizando estos nonce es posible repetir los paquetes y descifrarlos ya que la misma clave de descifrado se utiliza con valores nonce que ya se han utilizado en el pasado (reutilizando los llamados “keystream” cuando se cifran paquetes).
9. En función del análisis de los paquetes descifrados, sería posible insertar un programa malicioso en la red o simplemente analizar el tráfico generado por los usuarios de la red.

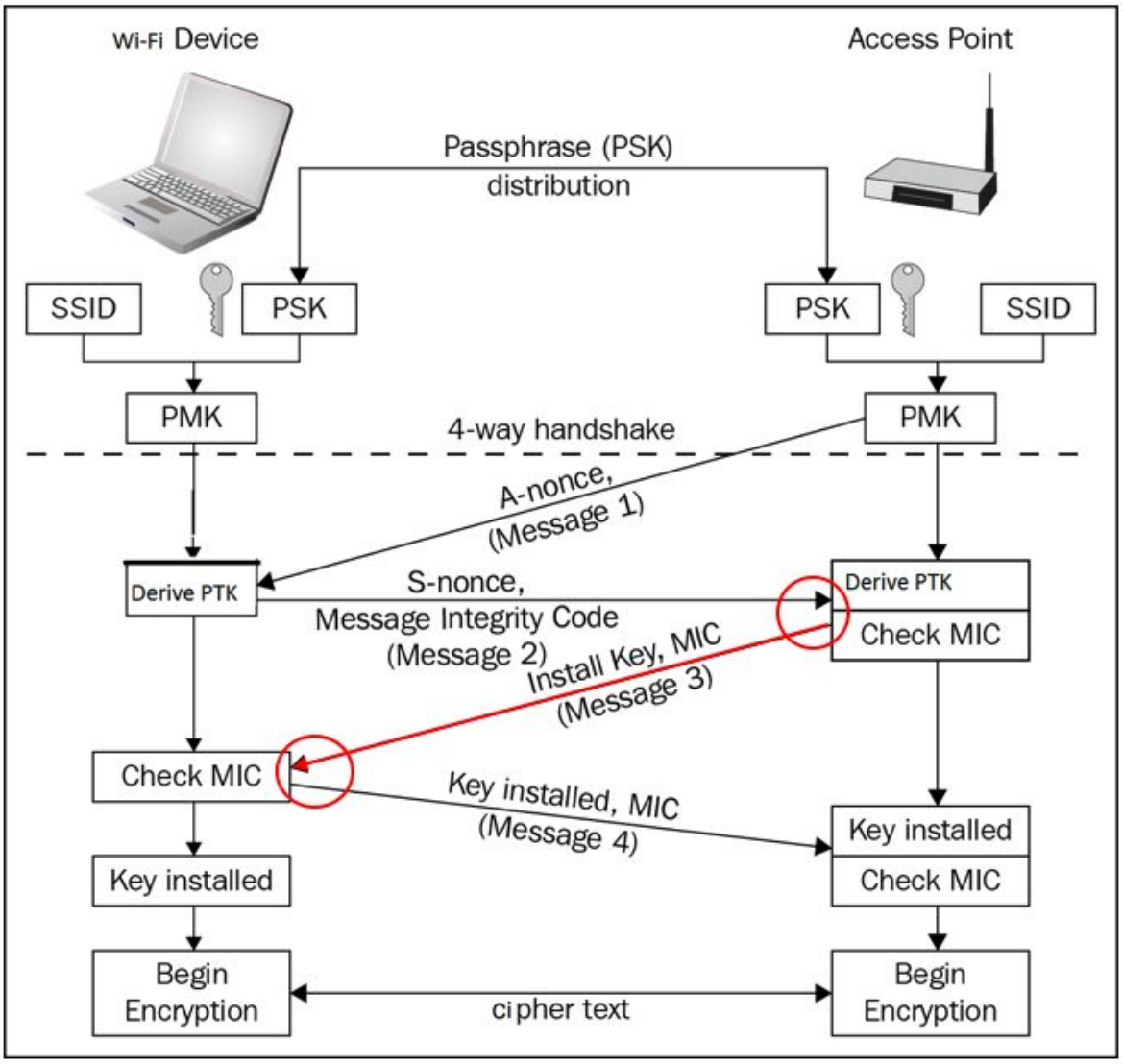


Figura 1: Flujo del proceso que realiza KRACK

DISPOSITIVOS Y PLATAFORMAS AFECTADOS

Prácticamente cualquier dispositivo que tenga WiFi tendrá que ser parcheado, desde dispositivos móviles pasando por routers.

Para más información sobre los dispositivos afectados y su estado puede verificar el siguiente LINK Vendors-KRACK-Vulnerables.

Fabricante	Estado	Fecha de Notificación	Fecha Actualización
Arch Linux	Afectado	28 Aug 2017	17-oct-17
Aruba Networks	Afectado	28 Aug 2017	9-oct-17
Broadcom	Afectado	30 Aug 2017	17-oct-17
Cisco	Afectado	28 Aug 2017	16-oct-17
Debian GNU/Linux	Afectado	28 Aug 2017	17-oct-17
Espressif Systems	Afectado	22-sept-17	13-oct-17
Extreme Networks	Afectado	28 Aug 2017	17-oct-17
Fedora Project	Afectado	28 Aug 2017	17-oct-17
Fortinet, Inc.	Afectado	28 Aug 2017	16-oct-17
FreeBSD Project	Afectado	28 Aug 2017	12-oct-17

Google	Afectado	28 Aug 2017	16-oct-17
HostAP	Afectado	30 Aug 2017	16-oct-17
Intel Corporation	Afectado	28 Aug 2017	10-oct-17
Juniper Networks	Afectado	28 Aug 2017	16-oct-17
Microchip Technology	Afectado	28 Aug 2017	16-oct-17

CVEs IDENTIFICADOS:

Los siguientes ID de CVE se han asignado para documentar estas vulnerabilidades en el protocolo WPA2:

CVE-ID	DESCRIPCIÓN
CVE-2017-13077	Reinstalación de la clave pairwise en el enlace de cuatro vías
CVE-2017-13078	Reinstalación de la clave de grupo en el enlace de cuatro vías
CVE-2017-13079	Reinstalación de la clave del grupo de integridad en el enlace de cuatro vías
CVE-2017-13080	Reinstalación de la clave de grupo en el apretón de manos de clave de grupo
CVE-2017-13081	Reinstalación de la clave de grupo de integridad en el apretón de manos de clave de grupo

CVE-2017-13082	Aceptar una Solicitud de Reasociación de Transición Rápida BSS retransmitida y volver a instalar la clave pairwise mientras la procesa
CVE-2017-13084	Reinstalación de la tecla STK en el apretón de manos PeerKey
CVE-2017-13086	Reinstalación de la clave de configuración de enlace directo Tunneled (TDLS) PeerKey (TPK) en el apretón de manos TDLS
CVE-2017-13087	Reinstalación de la clave de grupo (GTK) al procesar un marco de respuesta de modo de suspensión de gestión de red inalámbrica (WNM)
CVE-2017-13088	Reinstalación de la clave de grupo de integridad (IGTK) al procesar un marco de respuesta de modo de suspensión de gestión de red inalámbrica (WNM)

ACTUALIZACIONES

De momento esperar a que aparezca algún parche para cada uno de los dispositivos.

Nota: Cambiar de router o de contraseña de la WiFi no ayudará.

Actualizaciones de Seguridad

WINDOWS
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

FORTIGATE

- Para los modelos FortiGate Wifi usados bajo el modo Wifi Client:
  - Actualice a 5.6.2 compilación especial o próximo FortiOS 5.2.12, 5.4.6 o 5.6.3

NOTA: comuníquese con su TAC local para solicitar la compilación especial parcheada basada en FortiOS 5.6.2

- Para FortiAP utilizado como hoja de malla:
    - Actualice a FortiAP 5.6.1 o próximo FortiAP 5.2.7 o 5.4.4

CISCO

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa

Para más información de los parches disponibles puede visitar la siguiente página https://github.com/kristate/krackinfo

RECOMENDACIONES

Consejos y recomendaciones.

- Asegúrese de que siempre aparezca el ícono de un candado verde en la barra de tu navegador. Ese candado indica que se está usando una conexión HTTPS (cifrada y, por lo tanto, segura) en ese sitio web en particular. Si alguien intenta atacar con SSLstrip, el navegador se verá forzado a utilizar versiones HTTP de las páginas web, y el candado desaparecerá. Si el candado está en su sitio, su conexión es segura.

- Los investigadores advirtieron a algunos fabricantes de dispositivos de red (incluyendo a Wi-Fi Alliance, el cual es responsable de estandarizar los protocolos), antes de publicarlo, por lo que muchos de ellos deben estar en proceso de actualización de firmware para solucionar el problema con la reinstalación de clave. Así que, verifica si ya está disponible la actualización de firmware para tus dispositivos e instálala lo antes posible.

  https://char.gd/blog/2017/wifi-has-been-broken-heres-the-companies-that-have-already-fixed-it

- Puedes asegurar tu conexión utilizando una VPN, la cual añade otra capa de cifrado a los datos transferidos desde tu dispositivo.

- Filtrar las conexiones MAC del router para evitar que extraños entren en tu conexión.

REFERENCIAS

FUENTE PRINCIPAL:
https://www.krackattacks.com

PAPER:
https://papers.mathyvanhoef.com/ccs2017.pdf

FUENTES:
https://blogs.cisco.com/security/wpa-vulns
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080
https://www.kb.cert.org/vuls/id/228519

PoC:
https://www.youtube.com/watch?v=Oh4WURZoR98