BOLETÍN DE ALERTA

Boletín Nro.: 2017-15
Fecha de publicación: 16/10/2017
Tema: Vulnerabilidad crítica en WPA2 - Ataque KRACK

Sistemas afectados:

- Dispositivos WIFI que utilicen protocolo WPA2

Descripción:

Se ha descubierto una vulnerabilidad crítica que afecta a WPA2, el protocolo que protege el acceso a redes Wi-Fi modernas. La vulnerabilidad se debe a un error de diseño en el handshake de 4 vías del protocolo WPA2. El handshake se ejecuta cuando un cliente desea conectarse a una red Wi-Fi protegida y es utilizada para confirmar que tanto el cliente como el Access Point poseen las credenciales correctas, además de negociar una clave de encriptación nueva que será utilizada para encriptar todo el tráfico que posteriormente viajará por la red.

Un atacante que se encuentra dentro del rango de alcance de la víctima puede explotar dicha vulnerabilidad mediante una técnica de ataque denominada Reinstalación de claves (KRACKs - *Key Reinstallation Attacks*) que le permite leer información encriptada y descubrir información sensible. En este ataque, el atacante intenta que la víctima reinstale una clave de encriptación que ya está en uso, manipulando y retransmitiendo mensajes de handshake.

Normalmente, la instalación de la clave se da luego de recibir el tercer mensaje del handshake de 4 vías, con la cual encriptará el tráfico. Sin embargo, debido a que es posible que el mensaje se pierda, el access point es capaz de retransmitir el tercer mensaje si no recibe una respuesta de confirmación válida. Un atacante puede, de forma intencionada, lograr la pérdida de la confirmación de modo a que el AP retransmita el mensaje 3, con la misma clave. Debido al error en el diseño, es posible resetear los parámetros asociados tales como el contador de paquete transmitido (*nonce*) y de paquete recibido (*replay counter*) por lo que es posible la reutilización de la clave.

El ataque puede ser utilizado contra cualquier red Wi-Fi que utilice dicho protocolo, ya que se trata de una vulnerabilidad del propio protocolo y no de productos o implementaciones. La vulnerabilidad ha sido demostrada en productos Windows, Linux, Apple, Android, OpenBSD, MediaTek, Linksys y otros. Dependiendo de la configuración de la red, es posible inyectar y manipular datos. El ataque ha sido demostrado tanto contra redes Wi-Fi personales como del tipo Enterprise, así como también contra el protocolo más antiguo, WPA, que ya se encontraba roto por otras vulnerabilidades, y también contra redes que utilizan solo AES.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

El investigador que descubrió la vulnerabilidad notificó al CERT/CC, quien a su vez notificó a los actores involucrados, entre ellos la Wi-Fi Alliance y a los fabricantes de productos afectados. La notificación para fabricantes de productos wifi fue difundida el 28 de agosto, fecha desde la cual la mayoría ha trabajado en actualizaciones que corrigen la vulnerabilidad.

Detección:

La gran mayoría de los productos que soportan Wi-Fi están afectados. Una lista extensa pero no exhaustiva puede ser encontrada aquí:

https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

El investigador que descubrió la vulnerabilidad ha publicado un script para verificar la vulnerabilidad, sin embargo no la ha publicado todavía, a la espera de que las personas tengan un tiempo razonable para actualizar sus productos.

Impacto:

Un cibercriminal dentro del alcance de la cobertura Wi-Fi de un Access Point (AP) vulnerable puede conectarse a la misma arbitrariamente, pudiendo interceptar tráfico confidencial. Dependiendo del escenario, podría realizar ataques de inyección de distintos tipos, desde la red local vulnerada.

Mitigación y Solución:

Las vulnerabilidades fueron corregidas mediante actualizaciones de muchos fabricantes, entre ellos:

- OpenBSD
- Arch Linux
- Aruba
- Mikrotik
- Debian/Ubuntu
- Microsoft
- Ubiquiti
- Netgear:
  - WAC120, WAC505/WAC510, WAC720/730, WN604, WNAP210v2, WNAP320, WNDAP350, WNDAP620, WNDAP660, WND930

Se espera que otros fabricantes publiquen parches próximamente. Debe tenerse en cuenta que, en muchos casos, especialmente equipos de networking como routers, es necesario instalar el nuevo firmware de forma manual.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Puede ver la lista extensa de fabricantes para conocer el estado de la vulnerabilidad en cada uno de sus productos:
https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

De ninguna manera se recomienda utilizar otros protocolos como WEP, que, a pesar de no estar afectado por la presente vulnerabilidad, se encuentra roto. Se debe tener en cuenta que la vulnerabilidad que afecta a WPA2 es independiente de la elección de la contraseña, por lo que cambiarla y/o reforzarla no será suficiente para prevenir el ataque.

Información adicional:
https://www.krackattacks.com/
https://www.kb.cert.org/vuls/id/228519
https://papers.mathyvanhoef.com/ccs2017.pdf
https://www.windowscentral.com/vendors-who-have-patched-krack-wpa2-wi-fi-vulnerability

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py