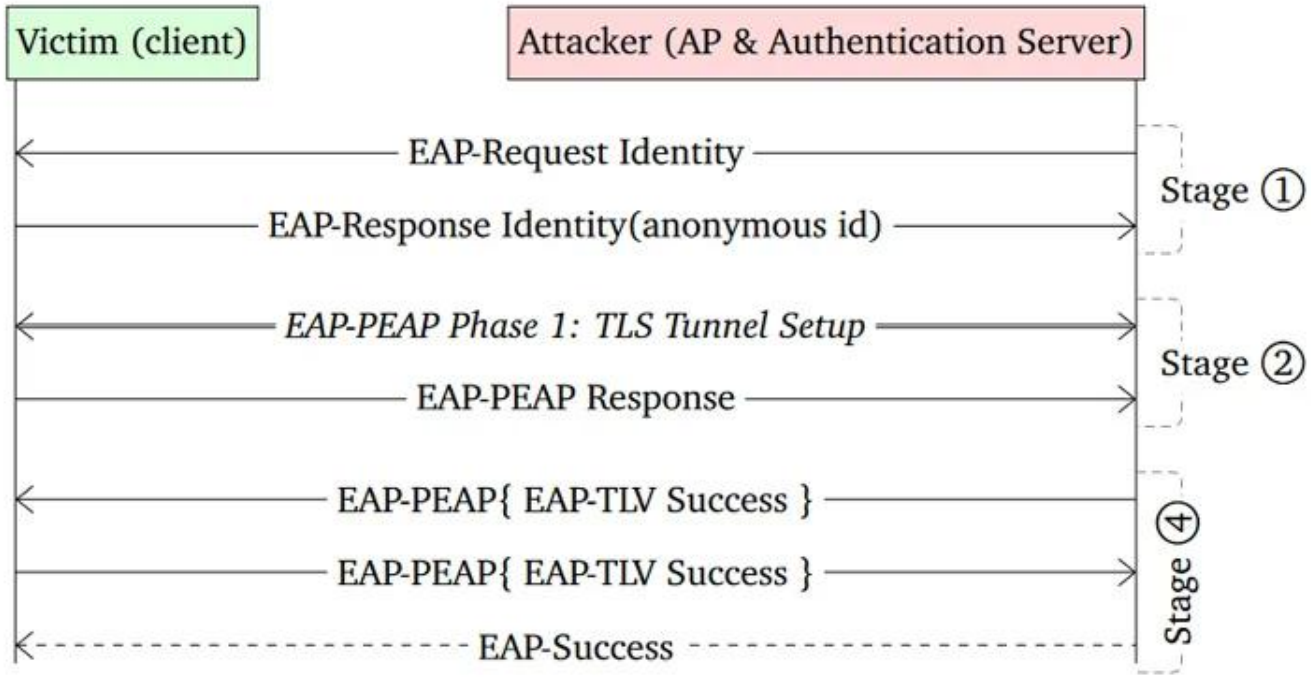
Investigadores en ciberseguridad han descubierto dos fallos de omisión de autenticación en el software Wi-Fi de código abierto presente en dispositivos Android, Linux y ChromeOS. Estas vulnerabilidades podrían engañar a los usuarios para unirse a una réplica maliciosa de una red legítima o permitir que un atacante acceda a una red confiable sin necesidad de contraseña.

Las debilidades, identificadas como CVE-2023-52160 y CVE-2023-52161, fueron encontradas durante una evaluación de seguridad de wpa_supplicant e Intel's iNet Wireless Daemon (IWD), respectivamente.

> Estos defectos *«posibilitan que los atacantes engañen a las víctimas para que se conecten a duplicados maliciosos de redes confiables e intercepten su tráfico, y se unan a redes seguras sin necesidad de contraseña»*, según un nuevo informe de investigación realizado en colaboración entre Top10VPN y Mathy Vanhoef, conocido por descubrir ataques Wi-Fi como KRACK, DragonBlood y TunnelCrack.

Especialmente, CVE-2023-52161 permite a un adversario obtener acceso no autorizado a una red Wi-Fi protegida, exponiendo a usuarios y dispositivos existentes a posibles amenazas como infecciones de malware, robo de datos y compromiso del correo electrónico empresarial (BEC). Este afecta a las versiones de IWD 2.12 y anteriores.

En cambio, CVE-2023-52160 impacta a las versiones de wpa_supplicant 2.10 y anteriores. Este es más crítico de los dos debido a que es el software predeterminado utilizado en dispositivos Android para manejar solicitudes de inicio de sesión en redes inalámbricas.



No obstante, solo afecta a clientes de Wi-Fi que no estén configurados adecuadamente para verificar el certificado del servidor de autenticación. Por otro lado, CVE-2023-52161 afecta a cualquier red que utilice un dispositivo Linux como punto de acceso inalámbrico (WAP).

La explotación exitosa de CVE-2023-52160 depende de que el atacante tenga el SSID de una red Wi-Fi a la que la víctima se haya conectado previamente, y también requiere que el actor de amenazas esté en proximidad física a la víctima.

> *«Un escenario posible podría ser que un atacante recorra el edificio de una empresa buscando redes antes de dirigirse a un empleado que sale de la oficina»,* señalaron los investigadores.

Distribuciones importantes de Linux, como Debian (1, 2), Red Hat (1), SUSE (1, 2) y Ubuntu

(1, 2), han emitido avisos sobre los dos fallos. El problema de wpa_supplicant también se ha solucionado en ChromeOS a partir de las versiones 118 y posteriores, pero aún no hay correcciones disponibles para Android.

> *«Mientras tanto, es esencial que los usuarios de Android configuren manualmente el certificado CA de cualquier red empresarial guardada para prevenir el ataque»,* advirtió Top10VPN.