



Dispositivos Android Xiaomi tienen múltiples vulnerabilidades en aplicaciones y componentes del sistema

Se han descubierto numerosas vulnerabilidades de seguridad en diversas aplicaciones y componentes del sistema presentes en los dispositivos Xiaomi que utilizan el sistema operativo Android.

Según un [informe](#) compartido por parte de la firma de seguridad móvil Oversecured, estas vulnerabilidades en Xiaomi permitían acceder a actividades, receptores y servicios arbitrarios con privilegios de sistema, así como robar archivos arbitrarios con los mismos privilegios, y divulgar información sobre teléfonos, configuraciones y cuentas Xiaomi.

Estas 20 debilidades afectan a diferentes aplicaciones y componentes, tales como:

- Galería (com.miui.gallery)
- GetApps (com.xiaomi.mipicks)
- Mi Video (com.miui.videoplayer)
- MIUI Bluetooth (com.xiaomi.bluetooth)
- Servicios de Teléfono (com.android.phone)
- Enviador de Impresión (com.android.printspooler)
- Seguridad (com.miui.securitycenter)
- Componente Principal de Seguridad (com.miui.securitycore)
- Configuraciones (com.android.settings)
- ShareMe (com.xiaomi.midrop)
- Seguimiento del Sistema (com.android.traceur), y
- Nube Xiaomi (com.miui.cloudservice)

Algunas de las falencias más destacadas incluyen una vulnerabilidad de inyección de comandos en la aplicación de Seguimiento del Sistema, así como fallas en la aplicación de Configuraciones que podrían facilitar el robo de archivos arbitrarios, y la divulgación de información sobre dispositivos Bluetooth, redes Wi-Fi conectadas y contactos de emergencia.

Es importante tener en cuenta que, aunque Servicios de Teléfono, Enviador de Impresión, Configuraciones y Seguimiento del Sistema son componentes legítimos del Proyecto de Código Abierto de Android ([AOSP](#)), han sido modificados por el fabricante de teléfonos chino



Dispositivos Android Xiaomi tienen múltiples vulnerabilidades en aplicaciones y componentes del sistema

para añadir funcionalidades adicionales, lo que ha resultado en estas vulnerabilidades.

También se ha encontrado una [vulnerabilidad de corrupción de memoria](#) en la aplicación GetApps, que a su vez se origina en una biblioteca de Android llamada [LiveEventBus](#). Oversecured reportó este problema a los responsables del proyecto hace más de un año, pero hasta la fecha no se ha solucionado.

La aplicación Mi Video ha sido descubierta utilizando [intenciones implícitas](#) para enviar información de cuentas Xiaomi, como nombre de usuario y dirección de correo electrónico, a través de [emisiones](#), lo que podría ser interceptado por cualquier aplicación de terceros instalada en los dispositivos mediante sus propios receptores de emisión.

Oversecured informó sobre estas vulnerabilidades a Xiaomi en un período de cinco días, del 25 al 30 de abril de 2024. Se recomienda a los usuarios que instalen las últimas actualizaciones disponibles para mitigar posibles amenazas.