

Alerta ID:	122
Fecha del reporte:	09/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidad crítica de ejecución remota de código (RCE) y escalamiento de privilegios en Android (CVE-2026-0073) permite a un atacante obtener acceso remoto como usuario shell mediante el bypass del mecanismo de autenticación de Wireless ADB, comprometiendo la confidencialidad, integridad y disponibilidad de dispositivos Android utilizados por organizaciones del sector salud.
Herramienta de detección	N/A
Activo involucrado:	Dispositivos Android utilizados en entornos hospitalarios, tabletas clínicas, teléfonos corporativos, dispositivos de autenticación multifactor (MFA), terminales móviles utilizados por personal asistencial, dispositivos biomédicos basados en Android, estaciones móviles de enfermería, equipos para telemedicina, terminales de captura de información clínica, dispositivos para rondas médicas, sistemas de movilidad empresarial (EMM/MDM), aplicaciones de Historia Clínica Electrónica (HCE), plataformas de interoperabilidad clínica, dispositivos IoT médicos basados en Android y cualquier equipo que ejecute versiones vulnerables del sistema operativo Android con el servicio Wireless ADB habilitado o susceptible de ser explotado mediante la vulnerabilidad CVE-2026-0073.
Tipo de alerta:	Alerta
Nivel de riesgo:	Crítico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la vulnerabilidad crítica CVE-2026-0073, identificada en el mecanismo de autenticación del servicio Wireless Android Debug Bridge (Wireless ADB) del sistema operativo Android, la cual permite que un actor de

amenaza obtenga acceso remoto al dispositivo sin requerir autenticación previa ni interacción por parte del usuario.

La explotación de esta vulnerabilidad posibilita el establecimiento de sesiones remotas con privilegios correspondientes al usuario shell, facilitando posteriormente la ejecución de comandos, el reconocimiento del dispositivo, la extracción de información, el despliegue de herramientas maliciosas y el desarrollo de actividades orientadas al compromiso progresivo del sistema.

La vulnerabilidad representa un escenario de riesgo significativo debido a que rompe uno de los mecanismos fundamentales de protección implementados para restringir el acceso remoto mediante Android Debug Bridge. Como consecuencia, un atacante ubicado dentro del mismo segmento de red o con capacidad para establecer comunicación hacia el dispositivo vulnerable puede eludir el proceso de autenticación normalmente requerido para iniciar una sesión ADB, obteniendo acceso administrativo sobre diversos componentes del sistema operativo sin necesidad de credenciales válidas ni aprobación del usuario.

Desde la perspectiva de la ciberseguridad, esta condición facilita el desarrollo de múltiples fases posteriores del ciclo de ataque. Una vez establecida la sesión remota, el actor malicioso puede realizar actividades de reconocimiento interno, enumeración del dispositivo, identificación de aplicaciones instaladas, recopilación de información sensible, manipulación de configuraciones de seguridad, despliegue de herramientas adicionales y utilización del dispositivo comprometido como punto de apoyo para comprometer otros activos tecnológicos pertenecientes a la organización.

El riesgo adquiere una relevancia particular para las entidades del sector salud, donde el uso de dispositivos Android se ha incrementado considerablemente como consecuencia de los procesos de transformación digital, movilidad clínica y prestación de servicios asistenciales. Actualmente, hospitales, clínicas, laboratorios, centros de diagnóstico, entidades promotoras de salud y proveedores tecnológicos utilizan dispositivos Android para soportar actividades relacionadas con Historia Clínica Electrónica (HCE), captura de información clínica, autenticación multifactor, telemedicina, visitas domiciliarias, gestión de inventarios, administración de dispositivos biomédicos, consulta de resultados diagnósticos, interoperabilidad clínica y acceso seguro a plataformas institucionales.

La explotación exitosa de esta vulnerabilidad podría permitir que un actor de amenaza obtenga acceso a información clínica almacenada localmente, intercepte procesos de autenticación, manipule configuraciones del dispositivo, comprometa aplicaciones corporativas, afecte la disponibilidad de servicios móviles críticos o utilice el equipo comprometido como punto de entrada hacia la infraestructura tecnológica institucional.

En escenarios donde los dispositivos mantienen conexiones permanentes con plataformas hospitalarias, redes inalámbricas corporativas o servicios de identidad institucional, el impacto puede extenderse más allá del dispositivo inicialmente comprometido, incrementando el riesgo para la confidencialidad, integridad y disponibilidad de la información institucional.

El propósito de esta alerta es que las organizaciones del sector salud identifiquen oportunamente los dispositivos potencialmente afectados, evalúen la exposición de los servicios Wireless ADB dentro de su infraestructura tecnológica, implementen las actualizaciones de seguridad publicadas por el fabricante y fortalezcan sus controles de monitoreo, detección y respuesta frente a posibles intentos de explotación.

De igual manera, se busca promover la adopción de medidas preventivas que reduzcan la superficie de ataque de los dispositivos Android utilizados para soportar procesos asistenciales, administrativos y de interoperabilidad clínica, contribuyendo a preservar la continuidad operacional y la seguridad de los servicios digitales del sector salud.

Descripción:

La vulnerabilidad **CVE-2026-0073** corresponde a una falla crítica de seguridad identificada en el mecanismo de autenticación implementado por **Wireless Android Debug Bridge (Wireless ADB)**, componente del sistema operativo Android que permite establecer sesiones remotas de depuración y administración sobre dispositivos mediante conexiones TCP/IP. La vulnerabilidad permite que un actor de amenaza eluda el proceso de autenticación requerido para establecer una sesión ADB inalámbrica, obteniendo acceso remoto al dispositivo con los privilegios asignados al usuario **shell**, sin requerir interacción del usuario ni conocimiento previo de credenciales válidas.

Android Debug Bridge (ADB) constituye una de las principales herramientas utilizadas por desarrolladores, fabricantes y administradores para realizar tareas de diagnóstico, mantenimiento, instalación de aplicaciones, recopilación de registros, ejecución de comandos y administración remota de dispositivos Android. Tradicionalmente, las conexiones ADB requerían acceso físico mediante interfaz USB; sin embargo, las versiones recientes del sistema operativo incorporaron la funcionalidad **Wireless ADB**, la cual permite establecer sesiones remotas utilizando redes IP, facilitando las labores de administración sobre dispositivos distribuidos geográficamente.

Para reducir los riesgos inherentes a la exposición remota de este servicio, Google implementó mecanismos de autenticación basados en el intercambio de claves criptográficas y procesos de emparejamiento (*pairing*), garantizando que únicamente clientes previamente autorizados pudieran establecer sesiones de administración remota. No obstante, la vulnerabilidad **CVE-2026-0073** introduce una condición que permite omitir dichos controles de autenticación bajo determinadas circunstancias, posibilitando que un cliente remoto especialmente preparado obtenga acceso al servicio ADB sin completar correctamente el proceso de autorización.

Desde una perspectiva técnica, la vulnerabilidad se origina en el procesamiento incorrecto de determinadas solicitudes durante el establecimiento de la sesión de depuración inalámbrica. Un atacante con capacidad para comunicarse con el dispositivo vulnerable puede manipular la secuencia de mensajes intercambiados durante el proceso de autenticación, induciendo al servicio Wireless ADB a aceptar una conexión no autorizada. Como resultado, el sistema crea una sesión remota válida asociada al usuario **shell**, permitiendo la ejecución de comandos sobre el dispositivo comprometido.

El usuario **shell** en Android dispone de privilegios significativamente superiores a los otorgados a las aplicaciones convencionales. Aunque no corresponde al usuario **root**, este contexto de ejecución permite acceder a una amplia variedad de interfaces administrativas del sistema operativo, ejecutar utilidades internas, consultar información del dispositivo, instalar aplicaciones mediante ADB, recopilar registros del sistema, modificar determinadas configuraciones, interactuar con servicios internos y ejecutar procesos adicionales que pueden facilitar posteriores actividades de escalamiento de privilegios o movimiento lateral.

La disponibilidad pública de una **Prueba de Concepto (Proof of Concept – PoC)** incrementa considerablemente el riesgo asociado a esta vulnerabilidad. Una vez divulgados los detalles

técnicos del mecanismo de explotación, actores de amenaza con capacidades limitadas pueden adaptar rápidamente herramientas automatizadas para identificar dispositivos vulnerables y ejecutar ataques a gran escala. Este escenario reduce significativamente la complejidad requerida para explotar la vulnerabilidad y aumenta la probabilidad de que sea incorporada en campañas dirigidas contra organizaciones públicas y privadas.

Uno de los aspectos más relevantes de esta vulnerabilidad corresponde a la ausencia de interacción por parte del usuario. A diferencia de numerosos ataques dirigidos contra dispositivos móviles, donde resulta necesario persuadir a la víctima para instalar aplicaciones maliciosas, aceptar permisos o interactuar con enlaces fraudulentos, **CVE-2026-0073** puede ser explotada sin que el propietario del dispositivo realice ninguna acción. Esta característica clasifica el escenario como un ataque **Zero-Click**, incrementando significativamente su criticidad desde la perspectiva de la gestión del riesgo.

Una vez obtenida la sesión ADB, el atacante puede desarrollar diversas actividades posteriores orientadas al compromiso progresivo del dispositivo. Entre ellas se incluyen el reconocimiento del sistema operativo, la identificación de aplicaciones instaladas, la recopilación de información sobre usuarios configurados, la obtención de registros de diagnóstico, la instalación de componentes adicionales mediante paquetes APK, la modificación de parámetros de depuración y la utilización del dispositivo como plataforma para ejecutar acciones adicionales sobre la infraestructura tecnológica de la organización.

En organizaciones del sector salud, este escenario adquiere especial relevancia debido al creciente número de dispositivos Android utilizados para soportar procesos clínicos y administrativos. Actualmente, tabletas, teléfonos inteligentes, terminales móviles, dispositivos biomédicos basados en Android y estaciones portátiles son utilizados para acceder a plataformas de Historia Clínica Electrónica (HCE), registrar procedimientos clínicos, consultar resultados diagnósticos, ejecutar aplicaciones de telemedicina, administrar inventarios farmacéuticos, gestionar rondas médicas, operar soluciones de autenticación multifactor y facilitar procesos de interoperabilidad con otras entidades del ecosistema de salud.

La explotación de la vulnerabilidad sobre uno de estos dispositivos podría permitir el acceso no autorizado a información clínica almacenada localmente, credenciales temporales utilizadas por aplicaciones corporativas, tokens de autenticación, certificados digitales y otros elementos que posteriormente podrían facilitar el compromiso de sistemas adicionales pertenecientes a

la organización. Asimismo, un dispositivo comprometido podría utilizarse como punto de apoyo para realizar actividades de reconocimiento sobre redes inalámbricas institucionales, identificar otros dispositivos conectados e intentar explotar servicios expuestos dentro del entorno hospitalario.

Otro aspecto que incrementa el riesgo operativo corresponde al uso extendido de plataformas de **Enterprise Mobility Management (EMM)** y **Mobile Device Management (MDM)** dentro de organizaciones del sector salud. Aunque estas soluciones fortalecen la administración centralizada de dispositivos móviles, un atacante que obtenga acceso ADB sobre un dispositivo vulnerable podría intentar evadir determinados controles de administración, alterar configuraciones locales o interferir con mecanismos utilizados para aplicar políticas de seguridad institucional.

La vulnerabilidad también representa un riesgo importante para organizaciones que utilizan dispositivos Android como segundo factor de autenticación para acceder a plataformas críticas. La manipulación del dispositivo comprometido podría afectar procesos relacionados con autenticación multifactor, recepción de códigos de verificación, aplicaciones de autenticación basadas en certificados digitales o mecanismos de identidad federada utilizados para acceder a sistemas institucionales.

Aunque actualmente no existen evidencias públicas que indiquen campañas masivas dirigidas específicamente contra organizaciones del sector salud utilizando esta vulnerabilidad, la publicación del exploit funcional incrementa considerablemente la probabilidad de que actores de amenaza incorporen esta técnica dentro de campañas más amplias orientadas al compromiso de dispositivos móviles corporativos. Esta situación resulta especialmente relevante para organizaciones que permiten el acceso de dispositivos Android a redes internas mediante esquemas **BYOD (Bring Your Own Device)** o que administran grandes cantidades de dispositivos móviles distribuidos entre personal asistencial y administrativo.

Finalmente, esta vulnerabilidad evidencia la importancia de mantener actualizados los sistemas operativos móviles y de aplicar oportunamente los boletines de seguridad publicados por los fabricantes. En entornos donde cientos o miles de dispositivos Android soportan procesos clínicos esenciales, la implementación tardía de actualizaciones de seguridad puede ampliar significativamente la superficie de ataque de la organización y aumentar la

probabilidad de compromiso de activos que intervienen directamente en la prestación de servicios de salud.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-0073** puede generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de la información procesada por dispositivos Android utilizados dentro de organizaciones del sector salud. A diferencia de vulnerabilidades cuyo impacto se limita a la indisponibilidad de un servicio o a la divulgación parcial de información, este escenario permite que un actor de amenaza obtenga acceso remoto al dispositivo mediante el servicio **Wireless Android Debug Bridge (Wireless ADB)**, facilitando posteriormente el desarrollo de múltiples actividades orientadas al compromiso progresivo del sistema y de los activos tecnológicos con los cuales interactúa.

Uno de los principales impactos corresponde al establecimiento de una sesión remota con privilegios del usuario **shell**, permitiendo la ejecución de comandos administrativos sobre el dispositivo comprometido. Aunque este nivel de privilegios no equivale inicialmente al usuario **root**, proporciona acceso suficiente para realizar actividades de reconocimiento, recopilación de información, administración de aplicaciones, interacción con servicios internos del sistema operativo y ejecución de herramientas adicionales que pueden facilitar ataques posteriores orientados al escalamiento de privilegios o persistencia.

Desde una perspectiva operacional, el acceso obtenido mediante Wireless ADB permite al actor de amenaza realizar un inventario detallado del dispositivo comprometido. Entre otras actividades, puede identificar la versión del sistema operativo, el modelo del equipo, aplicaciones instaladas, servicios activos, procesos en ejecución, configuraciones de red, interfaces inalámbricas disponibles, usuarios configurados, certificados digitales instalados y diversos parámetros internos del sistema. Esta información resulta especialmente valiosa para planificar fases posteriores del ataque y seleccionar técnicas específicas de explotación compatibles con la configuración del dispositivo.

La vulnerabilidad también puede facilitar el acceso a información sensible almacenada localmente por aplicaciones corporativas. Numerosas aplicaciones utilizadas en organizaciones del sector salud almacenan temporalmente archivos, registros de auditoría, configuraciones,

tokens de autenticación, certificados digitales, credenciales de acceso, historiales de conexión y otros elementos que podrían ser utilizados para comprometer servicios institucionales adicionales. Aunque la explotación de **CVE-2026-0073** no garantiza automáticamente el acceso a toda esta información, el nivel de control obtenido sobre el dispositivo incrementa considerablemente la superficie de exposición de dichos activos.

En organizaciones que utilizan dispositivos Android para acceder a plataformas de Historia Clínica Electrónica (HCE), sistemas de laboratorio (LIS), plataformas RIS, PACS, aplicaciones de telemedicina o soluciones de interoperabilidad clínica, el compromiso del dispositivo puede afectar directamente la confidencialidad de la información médica procesada durante la atención de pacientes. Un atacante podría capturar información visible en pantalla, acceder a archivos temporales generados por aplicaciones clínicas o recopilar datos utilizados durante procesos de autenticación con plataformas institucionales.

Otro impacto relevante corresponde a la posibilidad de instalar aplicaciones adicionales utilizando las capacidades propias del servicio ADB. Un actor de amenaza que obtenga acceso remoto podría desplegar herramientas destinadas al reconocimiento, monitoreo, captura de información o establecimiento de mecanismos de persistencia, incrementando progresivamente el nivel de compromiso del dispositivo. Dependiendo de la arquitectura de seguridad implementada por la organización, estas herramientas podrían operar de forma temporal o permanecer activas hasta ser identificadas mediante procesos de monitoreo o respuesta a incidentes.

La disponibilidad de una sesión ADB también facilita la modificación de determinadas configuraciones del dispositivo. Un atacante puede alterar parámetros relacionados con opciones de desarrollador, configuraciones de depuración, permisos otorgados a determinadas aplicaciones, políticas locales de seguridad o parámetros de conectividad, generando condiciones que favorezcan ataques posteriores o dificulten la identificación temprana del compromiso.

Desde la perspectiva de la continuidad del negocio, el compromiso de dispositivos móviles utilizados durante procesos asistenciales puede afectar directamente la prestación de servicios clínicos. En numerosas instituciones de salud, médicos, enfermeros, personal de laboratorio y equipos administrativos utilizan dispositivos Android para consultar historias clínicas, registrar procedimientos, acceder a resultados diagnósticos, validar órdenes médicas, gestionar

inventarios farmacéuticos y comunicarse con otras plataformas institucionales. La indisponibilidad o pérdida de confianza sobre estos dispositivos puede obligar a la organización a activar procedimientos manuales, reemplazar equipos comprometidos o suspender temporalmente determinados procesos asistenciales.

El impacto también puede extenderse hacia la infraestructura tecnológica institucional. Un dispositivo Android comprometido y conectado a redes inalámbricas corporativas puede utilizarse como punto de reconocimiento para identificar otros activos tecnológicos, servicios expuestos, segmentos de red y dispositivos conectados. Aunque la vulnerabilidad no incorpora capacidades nativas de movimiento lateral, el acceso inicial puede facilitar campañas posteriores dirigidas contra otros componentes de la infraestructura tecnológica.

Las organizaciones que implementan soluciones **Bring Your Own Device (BYOD)** enfrentan un riesgo adicional. La coexistencia de dispositivos personales y corporativos dentro de la misma infraestructura inalámbrica incrementa la superficie de ataque y dificulta la aplicación homogénea de controles de seguridad. Un dispositivo vulnerable perteneciente a un colaborador podría convertirse en un punto de acceso inicial para actividades de reconocimiento dirigidas contra recursos institucionales.

Otro escenario de riesgo corresponde a la afectación de mecanismos de autenticación multifactor. Diversas organizaciones utilizan dispositivos Android para generar códigos de autenticación, almacenar certificados digitales o ejecutar aplicaciones de identidad federada. El compromiso del dispositivo podría facilitar la captura de información utilizada durante procesos de autenticación, reduciendo la efectividad de algunos controles de acceso implementados para proteger sistemas críticos.

La explotación de esta vulnerabilidad también incrementa la carga operativa de los equipos responsables de infraestructura, movilidad empresarial y ciberseguridad. Una vez identificado un dispositivo comprometido, resulta necesario ejecutar actividades de aislamiento, análisis forense, validación de integridad, restablecimiento del sistema operativo, revocación de credenciales, revisión de accesos y monitoreo de posibles compromisos adicionales, generando una demanda significativa de recursos técnicos y operacionales.

Desde la perspectiva regulatoria, el compromiso de dispositivos que procesen datos personales o información clínica puede derivar en incidentes de seguridad con implicaciones

legales relacionadas con la protección de datos personales, la confidencialidad de la información médica y el cumplimiento de obligaciones establecidas por la normativa colombiana aplicable al sector salud. Dependiendo de la información comprometida y del alcance del incidente, la organización podría verse obligada a activar procedimientos internos de gestión de incidentes, realizar evaluaciones de impacto y adoptar medidas correctivas adicionales.

La disponibilidad pública de una prueba de concepto funcional incrementa además el riesgo de explotación oportunista. Una vez divulgadas las técnicas necesarias para comprometer dispositivos vulnerables, es habitual que grupos de ciberdelincuencia adapten rápidamente herramientas automatizadas destinadas a identificar equipos expuestos y ejecutar ataques masivos, reduciendo significativamente el tiempo disponible para que las organizaciones implementen las actualizaciones de seguridad correspondientes.

En escenarios donde la vulnerabilidad sea utilizada como parte de campañas de ataque más amplias, el acceso inicial obtenido mediante Wireless ADB podría combinarse con otras vulnerabilidades de Android, herramientas de post-explotación o técnicas de escalamiento de privilegios para obtener un control más profundo del dispositivo comprometido. Aunque **CVE-2026-0073** constituye el punto de entrada inicial, su explotación puede convertirse en el primer paso de una cadena de ataque orientada al compromiso completo del dispositivo y, eventualmente, de la infraestructura tecnológica de la organización.

En escenarios de explotación exitosa, un actor de amenaza podría:

- Obtener acceso remoto al dispositivo mediante Wireless ADB sin requerir autenticación ni interacción del usuario.
- Ejecutar comandos administrativos con privilegios del usuario **shell**.
- Realizar actividades de reconocimiento detallado sobre el dispositivo comprometido.
- Recopilar información del sistema operativo, aplicaciones instaladas y configuraciones internas.
- Acceder a información temporal almacenada por aplicaciones corporativas y clínicas.
- Instalar aplicaciones adicionales o herramientas utilizadas durante la fase de post-explotación.
- Modificar configuraciones relacionadas con depuración, conectividad o administración del dispositivo.

- Utilizar el dispositivo comprometido como punto de reconocimiento hacia la infraestructura tecnológica institucional.
- Interferir con procesos clínicos soportados por dispositivos Android utilizados durante la atención de pacientes.
- Incrementar la carga operativa de los equipos responsables de movilidad empresarial, infraestructura y ciberseguridad.
- Facilitar fases posteriores de escalamiento de privilegios, persistencia o movimiento lateral cuando existan vulnerabilidades adicionales presentes en el dispositivo.
- Comprometer la confidencialidad de información clínica, administrativa o de autenticación procesada por aplicaciones móviles institucionales.

Aunque la explotación inicial de **CVE-2026-0073** no proporciona automáticamente privilegios **root** sobre el dispositivo, el acceso remoto obtenido mediante el usuario **shell** representa un nivel de compromiso suficientemente elevado para afectar la seguridad de los dispositivos Android utilizados por organizaciones del sector salud y facilitar el desarrollo de ataques posteriores con mayor impacto sobre la infraestructura tecnológica institucional.

Modo de explotación del ataque

Fase 1 – Reconocimiento e identificación de dispositivos Android vulnerables

La cadena de ataque inicia con actividades de reconocimiento orientadas a identificar dispositivos Android que puedan ser susceptibles de explotación mediante la vulnerabilidad CVE-2026-0073. A diferencia de otras campañas dirigidas contra aplicaciones web o servidores expuestos a Internet, en este escenario el objetivo principal consiste en localizar dispositivos móviles que tengan habilitado el servicio Wireless Android Debug Bridge (Wireless ADB) o que puedan ser inducidos a establecer comunicaciones compatibles con el mecanismo vulnerable.

Durante esta fase, el actor de amenaza desarrolla actividades destinadas a identificar equipos Android conectados a redes corporativas, inalámbricas o de acceso remoto. Dependiendo del escenario de ataque, estas actividades pueden realizarse desde la misma red local, mediante dispositivos previamente comprometidos, utilizando infraestructura inalámbrica cercana o aprovechando accesos obtenidos durante fases anteriores de una campaña más amplia.

Desde una perspectiva técnica, el reconocimiento puede apoyarse en herramientas de descubrimiento de activos, análisis de servicios TCP, identificación de dispositivos mediante protocolos de red, enumeración de servicios de depuración, fingerprinting del sistema operativo Android, análisis de banners, consultas DNS internas y observación del tráfico generado por soluciones de administración de dispositivos móviles (MDM/EMM).

En organizaciones del sector salud, esta fase puede revelar la existencia de teléfonos inteligentes corporativos, tabletas clínicas, estaciones móviles de enfermería, dispositivos biomédicos basados en Android, terminales de captura de información clínica, dispositivos de autenticación multifactor y equipos utilizados durante procesos de telemedicina o atención domiciliaria.

Las actividades realizadas durante esta fase pueden incluir:

- identificación de dispositivos Android conectados a la red institucional;
- descubrimiento de servicios Wireless ADB accesibles;
- fingerprinting de versiones del sistema operativo Android;
- identificación de dispositivos administrados mediante plataformas MDM o EMM;
- análisis de puertos y servicios asociados al protocolo ADB;
- recopilación de información mediante técnicas OSINT cuando existan dispositivos expuestos;
- elaboración del inventario de objetivos potencialmente vulnerables.

El objetivo consiste en identificar dispositivos Android que puedan ser comprometidos mediante la vulnerabilidad CVE-2026-0073.

Fase 2 – Preparación de la infraestructura de explotación

Una vez identificados los dispositivos objetivo, el actor de amenaza prepara la infraestructura que utilizará para ejecutar el ataque. Debido a que la vulnerabilidad afecta el proceso de autenticación implementado por Wireless ADB, resulta necesario disponer de un cliente especialmente preparado para aprovechar el bypass de autenticación descrito por la vulnerabilidad.

Esta infraestructura puede estar conformada por estaciones de trabajo controladas por el atacante, dispositivos Android previamente comprometidos, sistemas Linux especialmente configurados para ejecutar herramientas ADB modificadas o plataformas de automatización capaces de establecer múltiples conexiones simultáneas hacia dispositivos vulnerables.

En campañas más sofisticadas, el atacante puede integrar el exploit dentro de marcos automatizados de explotación, permitiendo ejecutar procesos masivos de identificación y compromiso de dispositivos vulnerables distribuidos entre múltiples organizaciones.

Las actividades realizadas durante esta fase pueden incluir:

- preparación del exploit público (PoC);
- configuración de herramientas ADB modificadas;
- automatización del proceso de autenticación fraudulenta;
- validación del funcionamiento del exploit;
- configuración de infraestructura para administrar múltiples dispositivos comprometidos;
- preparación de herramientas de post-explotación;
- verificación del entorno antes de iniciar la explotación.

El objetivo consiste en disponer de una infraestructura capaz de establecer sesiones Wireless ADB utilizando el mecanismo de bypass de autenticación.

Fase 3 – Explotación del mecanismo de autenticación Wireless ADB

Con la infraestructura preparada, el atacante inicia la explotación de la vulnerabilidad estableciendo comunicación con el dispositivo Android objetivo.

Durante esta etapa, el exploit manipula el flujo de autenticación implementado por Wireless ADB, provocando que el dispositivo acepte una conexión remota sin completar correctamente el proceso criptográfico de emparejamiento requerido por el sistema operativo.

Como consecuencia, el servicio ADB establece una sesión válida asociada al usuario shell, permitiendo el acceso remoto al dispositivo sin intervención del propietario y sin necesidad de credenciales previamente autorizadas.

Desde la perspectiva del sistema operativo, la sesión aparenta corresponder a una conexión legítima, dificultando la identificación inmediata del compromiso cuando no existen mecanismos avanzados de monitoreo.

Las actividades realizadas durante esta fase pueden incluir:

- establecimiento de conexión TCP hacia el servicio Wireless ADB;
- ejecución del bypass de autenticación;
- establecimiento de una sesión remota válida;
- apertura del canal ADB;
- validación de privilegios obtenidos;
- comprobación de acceso al usuario shell;
- inicio de la fase de post-explotación.

El objetivo consiste en obtener acceso remoto al dispositivo mediante una sesión Wireless ADB autenticada de forma fraudulenta.

Fase 4 – Reconocimiento interno del dispositivo comprometido

Una vez obtenida la sesión remota, el atacante desarrolla actividades de reconocimiento destinadas a comprender la configuración del dispositivo y seleccionar los siguientes pasos de la campaña.

Durante esta fase se recopila información relacionada con:

- versión del sistema operativo;
- nivel de parches de seguridad;
- arquitectura del procesador;
- aplicaciones instaladas;
- usuarios configurados;
- procesos activos;
- servicios del sistema;
- redes configuradas;
- certificados instalados;

- políticas MDM;
- configuraciones de depuración.

Esta información permite adaptar herramientas posteriores al entorno específico del dispositivo comprometido.

Las actividades realizadas durante esta fase pueden incluir:

- ejecución de comandos ADB;
- enumeración de aplicaciones;
- identificación de procesos;
- recopilación de logs;
- identificación de interfaces de red;
- análisis del almacenamiento;
- recopilación de información del dispositivo.

El objetivo consiste en obtener información suficiente para planificar actividades posteriores de compromiso.

Fase 5 – Post-explotación y consolidación del acceso

Después del reconocimiento inicial, el actor de amenaza utiliza la sesión obtenida para ampliar el nivel de compromiso del dispositivo.

Dependiendo del modelo, versión de Android y controles implementados por la organización, esta fase puede incluir la instalación de aplicaciones maliciosas, herramientas de administración remota, utilidades para captura de información, mecanismos temporales de persistencia o exploits adicionales destinados al escalamiento de privilegios.

En campañas dirigidas, el atacante puede combinar CVE-2026-0073 con otras vulnerabilidades conocidas para obtener privilegios root, desactivar controles de seguridad o acceder a áreas protegidas del sistema operativo.

Las actividades realizadas durante esta fase pueden incluir:

- instalación de APK maliciosos;
- despliegue de herramientas de administración remota;
- recopilación de credenciales;
- instalación de componentes de persistencia;
- utilización de exploits adicionales;
- preparación para movimiento lateral;
- ocultamiento parcial de actividades.

El objetivo consiste en consolidar el acceso obtenido y ampliar las capacidades del atacante sobre el dispositivo comprometido.

Fase 6 – Acceso a información institucional y movimiento lateral

Con el dispositivo comprometido, el atacante puede comenzar a interactuar con los recursos corporativos a los cuales el equipo tiene acceso legítimo.

En organizaciones del sector salud, esto puede incluir plataformas como:

- Historia Clínica Electrónica (HCE);
- sistemas HIS;
- RIS;
- PACS;
- LIS;
- aplicaciones de telemedicina;
- correo corporativo;
- aplicaciones MFA;
- plataformas de interoperabilidad clínica;
- servicios VPN;
- aplicaciones administrativas.

El dispositivo comprometido puede utilizarse además como punto de reconocimiento sobre la infraestructura institucional para identificar nuevos objetivos.

Las actividades realizadas durante esta fase pueden incluir:

- acceso a aplicaciones corporativas;
- recopilación de información clínica;
- identificación de otros activos tecnológicos;
- reconocimiento de redes internas;
- utilización de credenciales almacenadas;
- establecimiento de conexiones hacia otros servicios;
- preparación de nuevos compromisos.

El objetivo consiste en extender el impacto del incidente más allá del dispositivo inicialmente comprometido.

Fase 7 – Mantenimiento del acceso y evasión de la detección

La última fase del ataque está orientada a mantener el acceso sobre el dispositivo durante el mayor tiempo posible y reducir la probabilidad de ser detectado por los mecanismos de monitoreo implementados por la organización.

Dependiendo de las capacidades obtenidas durante la post-explotación, el atacante puede eliminar registros temporales, finalizar procesos utilizados durante la explotación inicial, modificar configuraciones locales, desinstalar herramientas utilizadas durante el ataque o establecer mecanismos alternativos de acceso remoto que no dependan del servicio Wireless ADB.

En campañas avanzadas, el acceso inicial obtenido mediante CVE-2026-0073 puede convertirse únicamente en el primer paso de una operación persistente dirigida contra la infraestructura tecnológica de la organización.

Las actividades realizadas durante esta fase pueden incluir:

- eliminación de rastros de explotación;
- desactivación temporal de registros;
- establecimiento de nuevos canales de acceso;
- modificación de configuraciones locales;
- ocultamiento de herramientas desplegadas;

- mantenimiento del acceso remoto;
- preparación para futuras operaciones.

El objetivo consiste en preservar el acceso al dispositivo comprometido, dificultar la detección del incidente y facilitar el desarrollo de campañas posteriores contra la infraestructura tecnológica de la organización.

Vulnerabilidades asociadas

La vulnerabilidad CVE-2026-0073 corresponde a una falla crítica de bypass de autenticación que afecta el mecanismo de Wireless Android Debug Bridge (Wireless ADB). No obstante, desde la perspectiva de la respuesta a incidentes y la gestión de vulnerabilidades, este tipo de fallas rara vez son explotadas de forma aislada. En la mayoría de los escenarios, los actores de amenaza combinan el acceso inicial obtenido mediante esta vulnerabilidad con otras debilidades presentes en el sistema operativo Android, componentes del fabricante, aplicaciones empresariales o mecanismos de administración remota, incrementando progresivamente el nivel de compromiso sobre el dispositivo.

La combinación de varias vulnerabilidades permite construir cadenas de ataque más complejas, orientadas a obtener privilegios elevados, establecer persistencia, evadir mecanismos de seguridad, acceder a información sensible y utilizar el dispositivo comprometido como punto de apoyo para afectar otros activos tecnológicos de la organización.

A continuación, se describen las principales vulnerabilidades asociadas que pueden incrementar el impacto de CVE-2026-0073.

Bypass de autenticación (Authentication Bypass)

- **Descripción:** Las vulnerabilidades de Bypass de Autenticación permiten que un actor de amenaza eluda los mecanismos implementados para verificar la identidad de un usuario, dispositivo o servicio antes de conceder acceso a recursos protegidos. Estas vulnerabilidades suelen originarse por errores en la validación de credenciales, deficiencias en la implementación de protocolos de autenticación o fallas en los mecanismos de autorización.

En CVE-2026-0073, la vulnerabilidad afecta el proceso de autenticación de Wireless Android Debug Bridge (Wireless ADB), permitiendo establecer una sesión remota sin completar correctamente el proceso criptográfico de emparejamiento requerido por Android. Como consecuencia, el atacante obtiene acceso al dispositivo con privilegios correspondientes al usuario shell, sin requerir credenciales válidas ni interacción del usuario.

- **Impacto:** La explotación de este tipo de vulnerabilidades puede permitir:
 - Eludir completamente el proceso de autenticación.
 - Obtener acceso remoto no autorizado al dispositivo.
 - Ejecutar comandos administrativos mediante Android Debug Bridge.
 - Iniciar actividades de reconocimiento sobre el sistema comprometido.
 - Facilitar fases posteriores de post-explotación.
- **Relación con CVE-2026-0073:** Esta constituye la vulnerabilidad principal descrita en la presente alerta. La explotación exitosa de CVE-2026-0073 se basa precisamente en la omisión del mecanismo de autenticación implementado por Wireless ADB, permitiendo establecer una sesión remota sin autorización previa.
- **Referencias técnicas**
 - CWE-288 – Authentication Bypass Using an Alternate Path or Channel.
 - CWE-306 – Missing Authentication for Critical Function.
 - CAPEC-115 – Authentication Bypass.
- **MITRE ATT&CK**
 - T1190 – Exploit Public-Facing Application.
 - T1078 – Valid Accounts (cuando el bypass deriva en una sesión autenticada).

Escalamiento local de privilegios (Local Privilege Escalation)

- **Descripción:** Las vulnerabilidades de Escalamiento Local de Privilegios (LPE) permiten incrementar el nivel de permisos obtenidos inicialmente sobre un dispositivo hasta alcanzar privilegios administrativos o de root. Generalmente afectan el kernel de

Android, controladores (*drivers*), servicios privilegiados o componentes desarrollados por los fabricantes.

En Android, el usuario shell dispone de privilegios superiores a los de una aplicación convencional, lo que convierte el acceso inicial obtenido mediante CVE-2026-0073 en una excelente plataforma para ejecutar exploits adicionales orientados al escalamiento de privilegios.

- **Impacto:** La explotación puede permitir:
 - Obtener privilegios root.
 - Modificar componentes críticos del sistema operativo.
 - Desactivar controles de seguridad.
 - Acceder completamente al sistema de archivos.
 - Instalar malware persistente.
 - Comprometer totalmente el dispositivo.
- **Relación con CVE-2026-0073:** Aunque la vulnerabilidad no proporciona privilegios root, el acceso como usuario shell facilita la explotación de vulnerabilidades LPE presentes en el dispositivo, permitiendo al atacante obtener control total sobre Android.
- **Referencias técnicas**
 - CWE-269 – Improper Privilege Management.
 - CWE-250 – Execution with Unnecessary Privileges.
 - CAPEC-233 – Privilege Escalation.
- **MITRE ATT&CK**
 - T1068 – Exploitation for Privilege Escalation.

Ejecución remota de código (Remote Code Execution – RCE)

- **Descripción:** Las vulnerabilidades de Ejecución Remota de Código (RCE) permiten que un actor de amenaza ejecute instrucciones arbitrarias sobre un sistema objetivo desde una ubicación remota. Estas vulnerabilidades representan una de las categorías más

críticas dentro de la ciberseguridad debido a que permiten comprometer dispositivos sin requerir acceso físico.

En dispositivos Android, una sesión ADB obtenida mediante CVE-2026-0073 puede utilizarse para desplegar herramientas adicionales o explotar vulnerabilidades RCE presentes en aplicaciones del sistema, servicios privilegiados o componentes OEM.

- **Impacto:** La explotación puede permitir:
 - Ejecutar código arbitrario.
 - Instalar software malicioso.
 - Desplegar puertas traseras (*backdoors*).
 - Comprometer aplicaciones corporativas.
 - Alterar el funcionamiento del sistema operativo.
- **Relación con CVE-2026-0073:** El acceso inicial proporcionado por Wireless ADB facilita la preparación del entorno para la explotación de vulnerabilidades RCE adicionales, incrementando significativamente el nivel de compromiso del dispositivo.
- **Referencias técnicas**
 - CWE-94 – Improper Control of Generation of Code.
 - CWE-77 – Command Injection.
 - CAPEC-242 – Code Injection.
- **MITRE ATT&CK**
 - T1203 – Exploitation for Client Execution.
 - T1059 – Command and Scripting Interpreter.

Vulnerabilidades en componentes OEM de Android

- **Descripción:** Los fabricantes de dispositivos Android incorporan componentes propietarios, controladores, interfaces de administración, aplicaciones del sistema y servicios adicionales que complementan el sistema operativo base. Estos componentes pueden contener vulnerabilidades propias que permitan escalamiento de privilegios,

ejecución de código, evasión de controles de seguridad o acceso no autorizado al dispositivo.

Históricamente, múltiples campañas de ataque han aprovechado vulnerabilidades presentes en componentes OEM desarrollados por fabricantes como Samsung, Qualcomm, MediaTek, Xiaomi, Oppo y otros.

- **Impacto:** La explotación puede permitir:
 - Escalamiento de privilegios.
 - Acceso a firmware.
 - Compromiso del Trusted Execution Environment (TEE).
 - Persistencia.
 - Desactivación de controles de seguridad.
 - Compromiso permanente del dispositivo.
- **Relación con CVE-2026-0073:** Una vez obtenido acceso mediante Wireless ADB, un atacante puede identificar componentes OEM vulnerables y explotarlos para ampliar el nivel de compromiso del dispositivo.
- **Referencias técnicas**
 - CWE-119 – Improper Restriction of Operations within the Bounds of a Memory Buffer.
 - CWE-787 – Out-of-Bounds Write.
 - CAPEC-100 – Overflow Buffers.
- **MITRE ATT&CK**
 - T1068 – Exploitation for Privilege Escalation.
 - T1543 – Create or Modify System Process.

Vulnerabilidades en aplicaciones móviles empresariales

- **Descripción:** Las aplicaciones móviles utilizadas por organizaciones del sector salud pueden presentar vulnerabilidades relacionadas con almacenamiento inseguro de información, autenticación deficiente, exposición de credenciales, comunicaciones

inseguras, validación insuficiente de certificados o implementación incorrecta de mecanismos criptográficos.

Una vez comprometido el dispositivo mediante CVE-2026-0073, un actor de amenaza puede identificar aplicaciones vulnerables y utilizarlas para acceder a información clínica, credenciales corporativas, certificados digitales y otros recursos institucionales.

- **Impacto:** La explotación puede permitir:
 - Acceso a información clínica.
 - Robo de credenciales.
 - Exposición de tokens de autenticación.
 - Acceso no autorizado a sistemas institucionales.
 - Movimiento lateral.
 - Compromiso de procesos asistenciales.
- **Relación con CVE-2026-0073:** El acceso remoto obtenido mediante Wireless ADB incrementa la capacidad del atacante para analizar las aplicaciones instaladas en el dispositivo e identificar vulnerabilidades específicas que amplíen el alcance del incidente.
- **Referencias técnicas**
 - CWE-922 – Insecure Storage of Sensitive Information.
 - CWE-798 – Use of Hard-coded Credentials.
 - CWE-295 – Improper Certificate Validation.
 - CAPEC-37 – Retrieve Embedded Sensitive Data.
- **MITRE ATT&CK**
 - T1005 – Data from Local System.
 - T1555 – Credentials from Password Stores.
 - T1517 – Access Notifications.

Mapeo del Ataque a MITRE ATT&CK

La explotación de la vulnerabilidad **CVE-2026-0073** puede asociarse con diversas tácticas y técnicas descritas en el marco **MITRE ATT&CK®**, ampliamente utilizado por organizaciones de ciberseguridad para describir el comportamiento de actores de amenaza durante las diferentes fases de una campaña de ataque. Aunque esta vulnerabilidad corresponde específicamente a un **bypass del mecanismo de autenticación de Wireless Android Debug Bridge (Wireless ADB)**, su explotación puede formar parte de una cadena de ataque más amplia en la que el acceso inicial es utilizado para ejecutar actividades de reconocimiento, escalamiento de privilegios, recopilación de información, persistencia y movimiento lateral.

El mapeo presentado a continuación tiene como propósito facilitar que los equipos **SOC, CSIRT, Blue Team, Threat Hunting y Gestión de Vulnerabilidades** puedan comprender las técnicas potencialmente utilizadas por un atacante y desarrollar controles preventivos, reglas de correlación, casos de uso para plataformas SIEM y actividades de búsqueda proactiva de amenazas.

T1190 – Exploit Public-Facing Application

- **Descripción:** Esta técnica consiste en explotar vulnerabilidades presentes en servicios accesibles mediante la red para obtener acceso inicial al sistema objetivo. Aunque **Wireless ADB** normalmente no se encuentra expuesto a Internet, puede estar disponible dentro de redes corporativas, redes inalámbricas institucionales o entornos de desarrollo insuficientemente protegidos. Un atacante con acceso a la misma red podría aprovechar **CVE-2026-0073** para obtener acceso inicial al dispositivo.
- **Relación con la alerta:** Corresponde a la fase inicial del compromiso, donde el actor de amenaza aprovecha el bypass del mecanismo de autenticación para establecer una sesión remota con el dispositivo Android.

T1059 – Command and Scripting Interpreter

- **Descripción:** Una vez establecida la sesión mediante Wireless ADB, el atacante puede ejecutar comandos del sistema utilizando las capacidades administrativas proporcionadas por el usuario **shell**. Esto permite interactuar directamente con el sistema operativo, consultar información del dispositivo, ejecutar herramientas administrativas e iniciar actividades de post-explotación.
 - **Relación con la alerta:** El acceso proporcionado por **CVE-2026-0073** permite ejecutar comandos ADB que posteriormente pueden utilizarse para desplegar herramientas adicionales o preparar nuevas fases del ataque.
-

T1082 – System Information Discovery

- **Descripción:** Permite recopilar información relacionada con la configuración del dispositivo, versión del sistema operativo, arquitectura, fabricante, nivel de parches de seguridad y demás características técnicas que facilitan la planificación de ataques posteriores.
 - **Relación con la alerta:** Una vez comprometido el dispositivo, el atacante puede identificar rápidamente la versión de Android y determinar si existen vulnerabilidades adicionales susceptibles de explotación.
-

T1057 – Process Discovery

- **Descripción:** Consiste en identificar los procesos que se encuentran ejecutándose en el dispositivo para determinar aplicaciones activas, servicios privilegiados y componentes susceptibles de ser comprometidos.
 - **Relación con la alerta:** El acceso obtenido mediante Wireless ADB permite consultar procesos activos y comprender el funcionamiento interno del dispositivo antes de iniciar actividades de post-explotación.
-

T1016 – System Network Configuration Discovery

- **Descripción:** Permite obtener información relacionada con interfaces de red, direcciones IP, DNS configurados, rutas de comunicación y demás parámetros de conectividad.
 - **Relación con la alerta:** El atacante puede utilizar esta información para identificar otros activos tecnológicos accesibles desde el dispositivo comprometido.
-

T1068 – Exploitation for Privilege Escalation

- **Descripción:** Corresponde a la explotación de vulnerabilidades adicionales que permiten incrementar los privilegios inicialmente obtenidos sobre el sistema.
 - **Relación con la alerta:** Aunque **CVE-2026-0073** proporciona acceso como usuario **shell**, un atacante puede combinar este acceso con vulnerabilidades locales de escalamiento para obtener privilegios **root**.
-

T1543 – Create or Modify System Process

- **Descripción:** Permite crear, modificar o reutilizar procesos del sistema con el fin de mantener acceso persistente al dispositivo comprometido.
 - **Relación con la alerta:** Una vez comprometido el dispositivo, el atacante puede desplegar herramientas que permitan conservar el acceso aun cuando la sesión inicial de Wireless ADB haya finalizado.
-

T1547 – Boot or Logon Autostart Execution

- **Descripción:** Consiste en modificar mecanismos de inicio automático del sistema para ejecutar componentes maliciosos durante el arranque del dispositivo.

- **Relación con la alerta:** Puede utilizarse cuando el atacante obtiene privilegios elevados y busca mantener persistencia después del reinicio del dispositivo.
-

T1555 – Credentials from Password Stores

- **Descripción:** Consiste en acceder a credenciales almacenadas por aplicaciones o servicios presentes en el dispositivo.
 - **Relación con la alerta:** Dependiendo de las aplicaciones instaladas y del nivel de acceso obtenido, un atacante puede intentar recopilar credenciales, tokens de autenticación o certificados digitales utilizados para acceder a plataformas institucionales.
-

T1005 – Data from Local System

Descripción: Permite recopilar información almacenada localmente en el dispositivo comprometido.

Relación con la alerta: El atacante puede acceder a archivos temporales, registros, documentos, configuraciones, información clínica almacenada por aplicaciones móviles y otros datos sensibles.

T1021 – Remote Services

- **Descripción:** Consiste en utilizar el sistema comprometido para acceder posteriormente a otros recursos disponibles dentro de la infraestructura tecnológica.
 - **Relación con la alerta:** Un dispositivo Android comprometido puede convertirse en un punto de apoyo para identificar servicios corporativos, plataformas clínicas, aplicaciones internas y otros activos conectados a la misma red.
-

T1036 – Masquerading

- **Descripción:** Permite ocultar herramientas o procesos maliciosos simulando componentes legítimos del sistema operativo.
- **Relación con la alerta:** Durante la fase de post-explotación, un atacante puede intentar ocultar herramientas desplegadas en el dispositivo para reducir la probabilidad de detección.

La explotación de CVE-2026-0073 puede abarcar múltiples tácticas del marco MITRE ATT&CK, lo que evidencia que esta vulnerabilidad no debe considerarse únicamente como un problema de autenticación en dispositivos Android, sino como un posible vector de acceso inicial dentro de campañas de ataque dirigidas contra organizaciones del sector salud. Un dispositivo móvil comprometido puede utilizarse para acceder a aplicaciones clínicas, recopilar información sensible, comprometer credenciales institucionales e incluso servir como plataforma para ejecutar actividades de reconocimiento y movimiento lateral sobre la infraestructura tecnológica.

Por esta razón, se recomienda que las organizaciones utilicen este mapeo como referencia para fortalecer sus procesos de monitoreo, desarrollar reglas de detección en plataformas SIEM, orientar actividades de Threat Hunting y mejorar las capacidades de respuesta frente a incidentes relacionados con dispositivos móviles Android.

Recomendaciones

Con el propósito de reducir el riesgo de explotación de la vulnerabilidad **CVE-2026-0073** y fortalecer la seguridad de los dispositivos Android utilizados dentro de las organizaciones del sector salud, el **CSIRT Salud** recomienda implementar las siguientes medidas de prevención, detección, contención y fortalecimiento de la postura de ciberseguridad. Estas recomendaciones se encuentran alineadas con las mejores prácticas promovidas por **Google Android**, el **Android Security Bulletin**, el **NIST Cybersecurity Framework (CSF 2.0)**, las guías de seguridad para dispositivos móviles del **NIST**, el marco **MITRE ATT&CK** y los principios de **Zero Trust**.

Aplicar oportunamente las actualizaciones de seguridad

Las organizaciones deben identificar todos los dispositivos Android desplegados dentro de su infraestructura tecnológica y verificar que ejecuten las versiones del sistema operativo que incorporan las correcciones publicadas por Google para **CVE-2026-0073**. Los dispositivos que no reciban actualizaciones oficiales por parte del fabricante deben ser evaluados desde una perspectiva de riesgo y, cuando corresponda, retirados de la operación o reemplazados por equipos que cuenten con soporte vigente.

Asimismo, se recomienda validar que los fabricantes (OEM) hayan publicado los parches correspondientes para sus dispositivos, ya que en muchos casos las actualizaciones de seguridad son distribuidas por cada fabricante y no directamente por Google.

Deshabilitar Wireless Android Debug Bridge (Wireless ADB)

Wireless ADB únicamente debe permanecer habilitado cuando exista una necesidad técnica plenamente justificada y previamente autorizada.

El **CSIRT Salud** recomienda:

- Deshabilitar **Wireless Debugging** en todos los dispositivos utilizados para actividades asistenciales y administrativas.
- Restringir el uso de Android Debug Bridge exclusivamente al personal técnico autorizado.
- Deshabilitar las **Opciones de Desarrollador** una vez finalicen las actividades de soporte.
- Verificar periódicamente que el servicio ADB no permanezca habilitado de forma permanente.

Fortalecer la administración de dispositivos móviles (MDM/EMM)

Las plataformas de **Mobile Device Management (MDM)** y **Enterprise Mobility Management (EMM)** deben utilizarse como mecanismo principal para controlar la configuración de seguridad de los dispositivos Android.

Se recomienda implementar políticas que permitan:

- Impedir la activación de las Opciones de Desarrollador.
- Bloquear la habilitación de Wireless Debugging.
- Detectar modificaciones no autorizadas sobre la configuración del sistema.
- Impedir la instalación de aplicaciones fuera del catálogo corporativo.
- Verificar permanentemente el cumplimiento de las políticas de seguridad institucionales.

Implementar segmentación de red

Los dispositivos Android utilizados por la organización no deben compartir segmentos de red con servidores críticos, sistemas biomédicos o plataformas que soporten procesos asistenciales.

Se recomienda:

- Segmentar los dispositivos móviles mediante VLAN dedicadas.
- Limitar la comunicación únicamente hacia los servicios estrictamente necesarios.
- Implementar listas de control de acceso (ACL) para restringir conexiones administrativas.
- Bloquear el acceso al servicio Wireless ADB desde segmentos no autorizados.

Adoptar un modelo de Zero Trust para dispositivos móviles

Las organizaciones deben asumir que ningún dispositivo conectado a la red es confiable por defecto.

Por tal motivo, se recomienda implementar controles basados en el principio de **Zero Trust**, incluyendo:

- Verificación continua del estado de seguridad del dispositivo.
- Evaluación permanente del cumplimiento de políticas.

- Validación del nivel de actualización del sistema operativo.
 - Control del contexto de acceso antes de autorizar conexiones hacia plataformas institucionales.
 - Restricción automática del acceso cuando un dispositivo incumpla las políticas de seguridad.
-

Fortalecer el monitoreo de dispositivos Android

Los equipos responsables de ciberseguridad deben implementar mecanismos de monitoreo continuo que permitan identificar actividades compatibles con la explotación de **CVE-2026-0073**.

Se recomienda generar alertas cuando se detecten:

- Activación de Wireless Debugging.
 - Nuevas autorizaciones de clientes ADB.
 - Instalación remota de aplicaciones.
 - Cambios inesperados en las Opciones de Desarrollador.
 - Incremento de sesiones administrativas ADB.
 - Conexiones provenientes de estaciones de trabajo no autorizadas.
-

Fortalecer la gestión de vulnerabilidades

Las organizaciones deben incorporar los dispositivos Android dentro del proceso institucional de gestión de vulnerabilidades.

El **CSIRT Salud** recomienda:

- Mantener un inventario actualizado de todos los dispositivos Android.
- Verificar periódicamente el nivel de parches de seguridad.
- Priorizar la remediación de vulnerabilidades críticas.
- Validar permanentemente el estado de soporte de los dispositivos desplegados.

- Incorporar dispositivos móviles dentro de los procesos de evaluación de riesgos tecnológicos.
-

Restringir la instalación de aplicaciones

Las aplicaciones instaladas en dispositivos corporativos deben provenir exclusivamente de fuentes autorizadas por la organización.

Se recomienda:

- Restringir la instalación de APK desde orígenes desconocidos.
 - Utilizar únicamente Google Play administrado o repositorios corporativos autorizados.
 - Validar la integridad y autenticidad de las aplicaciones antes de su instalación.
 - Eliminar aplicaciones innecesarias que incrementen la superficie de ataque.
-

Implementar mecanismos de detección y respuesta

Las organizaciones que dispongan de plataformas **SIEM**, **XDR**, **EDR** o soluciones de monitoreo móvil deben desarrollar casos de uso específicos para identificar actividades relacionadas con Wireless ADB.

Se recomienda:

- Correlacionar eventos provenientes de Android, MDM, infraestructura inalámbrica y plataformas de autenticación.
 - Incorporar reglas específicas relacionadas con el proceso **adbd**.
 - Realizar actividades periódicas de **Threat Hunting** orientadas a identificar dispositivos comprometidos.
 - Integrar las alertas generadas por dispositivos móviles dentro del proceso institucional de gestión de incidentes.
-

Fortalecer la gestión de identidades y accesos

Los dispositivos Android utilizados para acceder a plataformas institucionales deben cumplir controles adicionales relacionados con autenticación y gestión de identidades.

El **CSIRT Salud** recomienda:

- Implementar autenticación multifactor resistente al phishing.
 - Utilizar certificados digitales administrados por la organización.
 - Revocar inmediatamente credenciales asociadas a dispositivos comprometidos.
 - Aplicar el principio de mínimo privilegio para todas las aplicaciones móviles.
-

Sensibilizar al personal técnico

Aunque **CVE-2026-0073** no requiere interacción del usuario para su explotación, resulta fundamental que el personal responsable de administrar dispositivos móviles conozca los riesgos asociados al uso de Wireless ADB.

Se recomienda desarrollar actividades periódicas de capacitación sobre:

- Riesgos asociados a Android Debug Bridge.
 - Configuración segura de dispositivos Android.
 - Gestión segura de dispositivos móviles corporativos.
 - Procedimientos para habilitar y deshabilitar Wireless Debugging.
 - Respuesta a incidentes relacionados con dispositivos móviles.
-

Recomendaciones específicas para el sector salud

Las entidades del sector salud deberían adoptar controles adicionales sobre los dispositivos Android utilizados durante la prestación de servicios asistenciales.

El **CSIRT Salud** recomienda:

- Verificar que los dispositivos utilizados para acceder a **Historias Clínicas Electrónicas (HCE)** ejecuten versiones actualizadas del sistema operativo Android.
- Impedir la habilitación de **Wireless Debugging** en tabletas clínicas, dispositivos biomédicos basados en Android y terminales móviles utilizados por el personal asistencial.
- Supervisar permanentemente los dispositivos administrados mediante plataformas MDM/EMM.
- Implementar segmentación de red para aislar dispositivos móviles de los sistemas clínicos críticos.
- Incorporar dispositivos Android dentro de los ejercicios periódicos de evaluación de vulnerabilidades y pruebas de respuesta a incidentes.
- Actualizar los procedimientos institucionales de gestión de incidentes para contemplar escenarios relacionados con la explotación de vulnerabilidades en dispositivos móviles.
- Verificar periódicamente el cumplimiento de las políticas institucionales sobre dispositivos móviles y administración remota.

Conclusiones

La vulnerabilidad **CVE-2026-0073** representa una amenaza crítica para la seguridad de los dispositivos Android al comprometer uno de los mecanismos diseñados para proteger el acceso remoto mediante **Wireless Android Debug Bridge (Wireless ADB)**. La posibilidad de eludir el proceso de autenticación y establecer una sesión administrativa sin requerir credenciales válidas ni interacción del usuario convierte esta vulnerabilidad en un vector de acceso inicial de alta criticidad, especialmente en entornos donde los dispositivos móviles forman parte de la infraestructura tecnológica que soporta procesos institucionales.

Desde la perspectiva de la ciberseguridad, el principal riesgo asociado a esta vulnerabilidad no radica únicamente en el acceso inicial al dispositivo, sino en la posibilidad de que dicho acceso sea utilizado como punto de partida para desarrollar campañas de ataque más complejas. Un actor de amenaza que obtenga acceso mediante **CVE-2026-0073** puede ejecutar actividades de reconocimiento, recopilar información sensible, instalar herramientas de post-explotación, explotar vulnerabilidades adicionales para obtener privilegios elevados y utilizar el dispositivo comprometido como plataforma para acceder a otros activos tecnológicos de la organización.

Para el sector salud, el impacto potencial adquiere una dimensión aún mayor debido al papel estratégico que desempeñan los dispositivos Android dentro de los procesos asistenciales y administrativos. Actualmente, estos dispositivos son utilizados para acceder a **Historias Clínicas Electrónicas (HCE)**, sistemas de información hospitalaria (**HIS**), plataformas de laboratorio (**LIS**), sistemas de imágenes diagnósticas (**RIS/PACS**), soluciones de telemedicina, plataformas de interoperabilidad, aplicaciones de autenticación multifactor y herramientas de movilidad clínica. El compromiso de cualquiera de estos dispositivos puede afectar la confidencialidad de la información clínica, la integridad de los procesos asistenciales y la disponibilidad de servicios esenciales para la atención de pacientes.

La publicación de una **Prueba de Concepto (Proof of Concept - PoC)** incrementa significativamente el nivel de riesgo asociado a esta vulnerabilidad. La disponibilidad pública de herramientas de explotación reduce la complejidad técnica requerida para llevar a cabo ataques exitosos y aumenta la probabilidad de que actores maliciosos incorporen esta vulnerabilidad dentro de campañas automatizadas dirigidas contra organizaciones públicas y privadas. En consecuencia, las entidades no deben esperar la confirmación de campañas activas para implementar las medidas de protección recomendadas, sino adoptar un enfoque preventivo basado en la gestión proactiva del riesgo.

La presente alerta también evidencia la importancia de fortalecer la seguridad de los dispositivos móviles como parte integral de la estrategia institucional de ciberseguridad. En muchos casos, los programas de gestión de vulnerabilidades concentran sus esfuerzos en servidores, estaciones de trabajo o aplicaciones corporativas, dejando en un segundo plano los dispositivos móviles. Sin embargo, el incremento del trabajo móvil, la telemedicina, las aplicaciones clínicas y las estrategias **Bring Your Own Device (BYOD)** han convertido a estos dispositivos en objetivos de alto valor para los actores de amenaza.

Las organizaciones del sector salud deben asumir que la protección de los dispositivos Android requiere una estrategia integral que combine la aplicación oportuna de actualizaciones de seguridad, el endurecimiento de la configuración del sistema operativo, la administración centralizada mediante soluciones **MDM/EMM**, la segmentación de red, la adopción de principios de **Zero Trust**, el monitoreo continuo de eventos de seguridad y el desarrollo de capacidades de detección y respuesta frente a incidentes relacionados con plataformas móviles.

Asimismo, resulta indispensable fortalecer los procesos institucionales de gestión de activos tecnológicos, garantizando que todos los dispositivos Android utilizados por la organización se encuentren debidamente inventariados, administrados, actualizados y sometidos a procesos periódicos de evaluación de vulnerabilidades. Los dispositivos que hayan alcanzado el fin de su ciclo de soporte o que no reciban actualizaciones de seguridad por parte del fabricante deben ser reemplazados oportunamente para evitar que se conviertan en puntos de entrada para ataques dirigidos contra la infraestructura institucional.

Finalmente, el **CSIRT Salud** recomienda a todas las entidades del sector realizar una evaluación inmediata de su nivel de exposición frente a **CVE-2026-0073**, verificando la configuración de **Wireless Android Debug Bridge**, identificando dispositivos potencialmente vulnerables, aplicando las actualizaciones publicadas por los fabricantes e incorporando los controles de monitoreo, detección y respuesta descritos en la presente alerta. La adopción temprana de estas medidas contribuirá significativamente a reducir la probabilidad de explotación de la vulnerabilidad, fortalecer la resiliencia operativa de las organizaciones y proteger la continuidad de los servicios de salud soportados por tecnologías móviles.

La protección de los dispositivos Android debe entenderse como un componente fundamental de la estrategia de seguridad digital del sector salud. En un entorno donde la movilidad, la interoperabilidad y la transformación digital continúan expandiendo la superficie de ataque, la gestión adecuada de las vulnerabilidades en plataformas móviles constituye un elemento esencial para preservar la **confidencialidad, integridad y disponibilidad** de la información clínica, garantizar la continuidad de la atención a los pacientes y fortalecer la capacidad de respuesta de las organizaciones frente a amenazas cibernéticas emergentes.

Fuentes:

- <https://source.android.com/docs/security/bulletin>
- <https://source.android.com/docs/security>
- <https://developer.android.com/tools/adb>
- <https://developer.android.com/studio/debug/dev-options#wireless>
- <https://source.android.com>
- <https://developer.android.com/privacy-and-security>
- <https://www.cve.org/>

- <https://www.cve.org/CVERecord?id=CVE-2026-0073>
- <https://nvd.nist.gov/>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-0073>
- <https://attack.mitre.org/>
- <https://attack.mitre.org/matrices/mobile/>
- <https://cwe.mitre.org/>
- <https://capec.mitre.org/>
- <https://www.nist.gov/cyberframework>
- <https://csrc.nist.gov/pubs/sp/800/124/r2/final>
- <https://csrc.nist.gov/pubs/sp/800/61/r2/final>
- <https://securityonline.info/android-remote-root-exploit/>
- <https://www.securityweek.com/critical-remote-code-execution-vulnerability-patched-in-android-2/>
- https://www.hkcert.org/security-bulletin/android-remote-code-execution-vulnerability_20260505
- <https://www.decryptiondigest.com/blog/android-cve-2026-0073-zero-click-adbd-rce>
- <https://securityaffairs.com/191710/breaking-news/critical-android-vulnerability-cve-2026-0073-fixed-by-google.html>
- <https://mas.owasp.org/MASVS/>
- <https://mas.owasp.org/MASTG/>
- <https://owasp.org/www-project-mobile-top-10/>
- <https://owasp.org/www-project-mobile-security-testing-guide/>
- <https://android-developers.googleblog.com/>
- <https://developer.android.com/docs>
- <https://source.android.com/docs/security/features>
- <https://androidenterprisepartners.withgoogle.com/devices/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.