

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.


Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Una vulnerabilidad crítica de Android que permite la ejecución sin clics posibilita el acceso remoto a la consola. 4

Índice alfabético 6

| | | | |
|---|--|------------------------------|-------------------|
|  | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°064 | | Fecha: 04-05-2026 |
| | | | Página: 4 de 6 |
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | Una vulnerabilidad crítica de Android que permite la ejecución sin clics posibilita el acceso remoto a la consola. | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

1. ANTECEDENTES:

En mayo de 2026, Google publicó el Android Security Bulletin, alertando sobre una vulnerabilidad crítica detectada en el componente central del sistema Android. Esta falla, clasificada como zero-click, no requiere interacción alguna del usuario para ser explotada, lo que incrementa significativamente su nivel de riesgo. La vulnerabilidad afecta versiones modernas de Android y fue corregida mediante parches de seguridad distribuidos directamente por Google, resaltando la creciente sofisticación de los ataques orientados a dispositivos móviles y la necesidad de reforzar los mecanismos de actualización oportuna.



Ilustración 1 Una vulnerabilidad crítica de Android que permite la ejecución sin clics posibilita el acceso remoto a la consola.

2. DETALLES:

La vulnerabilidad, identificada como CVE-2026-0073, reside en el componente Android System, específicamente en el submódulo Android Debug Bridge Daemon (adb) bajo Project Mainline. Un atacante ubicado en la misma red local o en proximidad física puede explotar esta falla para ejecutar código de manera remota y obtener acceso al dispositivo con privilegios de shell, sin que el usuario realice ninguna acción. Este acceso permite evadir protecciones de aislamiento, ejecutar comandos del sistema y potencialmente comprometer información sensible del dispositivo. La vulnerabilidad impacta equipos con Android 14, 15, 16 y 16-QPR2, y se mitiga aplicando el parche de seguridad con nivel 2026-05-01 o superior. Google ha indicado que, hasta el momento, no existen evidencias de explotación activa, aunque el vector de ataque es considerado de criticidad máxima.

3. RECOMENDACIONES:

- Actualizar inmediatamente los dispositivos Android al nivel de parche de seguridad 2026-05-01 o posterior.
- Evitar el uso de redes Wi-Fi públicas o no confiables, especialmente sin mecanismos de protección adicionales.
- Mantener habilitadas las actualizaciones automáticas del sistema y de Google Play System Updates.
- Implementar Mobile Device Management (MDM) en entornos corporativos para controlar versiones, parches y configuraciones.
- Deshabilitar ADB inalámbrico y funciones de depuración cuando no sean estrictamente necesarias.
- Utilizar soluciones de Mobile Threat Defense (MTD) y monitoreo continuo para detectar comportamientos anómalos.
- Fortalecer la concienciación en ciberseguridad móvil, destacando el riesgo de vulnerabilidades zero-click y la importancia del parchado oportuno.

Fuente de Información:

- <https://gbhackers.com/critical-android-zero-click-vulnerability/>

Índice alfabético

Explotación de vulnerabilidades conocidas 4