



PERÚ

Presidencia  
del Consejo de Ministros

Secretaría de Gobierno  
y Transformación Digital

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL



 Asociación de  
Bancos del Perú

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL

## 254-2025-CNSD

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

Vulnerabilidad Crítica de Ejecución Remota de Código en Dispositivos Android (CVE-2025-48593) .....	4
Vulnerabilidad crítica en el sistema Radiometrics VizAir.....	6
Vulnerabilidad en el software CNCSoft-G2 de Delta Electronics.....	7
Índice alfabético .....	8

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°254</b>		Fecha: 04-11-2025
			Página: 4 de 8
<b>Componente que reporta</b>	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad Crítica de Ejecución Remota de Código en Dispositivos Android (CVE-2025-48593)		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	Troyanos
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		

**Descripción**

**1. ANTECEDENTES:**

Google ha emitido una **alerta de seguridad urgente** tras identificar una vulnerabilidad crítica de **ejecución remota de código (RCE)** en el componente del sistema operativo Android. El fallo, identificado como **CVE-2025-48593**, afecta a las versiones **Android 13 hasta 16** y se considera una amenaza de alta peligrosidad debido a que **no requiere interacción del usuario** para su explotación. A diferencia de otros ataques que dependen de enlaces maliciosos o descargas sospechosas, esta vulnerabilidad puede ser aprovechada de manera **silenciosa**, permitiendo que un atacante ejecute código malicioso de forma remota sin intervención del propietario del dispositivo. Google ha calificado el nivel de severidad como **“crítico”**, señalando que su explotación podría comprometer completamente el control de los dispositivos afectados.



*Ilustración 1: Vulnerabilidad Android (Fuente:GBHackers.com)*

**2. DETALLES:**

La vulnerabilidad **CVE-2025-48593** se origina en un **componente central del sistema Android**, lo que amplía considerablemente el número de dispositivos potencialmente vulnerables. Entre los principales aspectos técnicos y operativos de este incidente se destacan:

- **Tipo de vulnerabilidad:** Ejecución remota de código (Remote Code Execution, RCE).
- **Grado de severidad:** Crítico, según la evaluación oficial de Google.
- **Versiones afectadas:** Android 13, 14, 15 y 16.
- **Interacción del usuario:** No requerida; la explotación puede realizarse de forma remota.
- **Impacto potencial:** Control total del dispositivo comprometido, incluso sin privilegios elevados.
- **Mitigaciones iniciales:** Publicación de parches de seguridad en el **Android Open Source Project (AOSP)** el 1 de noviembre de 2025.

Google notificó a sus socios fabricantes **con un mes de anticipación**, con el propósito de que desarrollaran las actualizaciones correspondientes. Sin embargo, los dispositivos que no hayan recibido la **actualización de seguridad con fecha 2025-11-01 o posterior** continúan en situación de riesgo.

El boletín de seguridad también incluye la vulnerabilidad **CVE-2025-48581**, catalogada como de **alta severidad**, aunque con menor impacto inmediato que la RCE principal.

### 3. RECOMENDACIONES:


Dado el alcance global y la criticidad del fallo, se recomienda que tanto fabricantes como usuarios adopten medidas inmediatas para mitigar los riesgos asociados:


- **Actualizar los dispositivos Android** a la versión más reciente disponible, asegurando que el nivel de parche de seguridad sea **2025-11-01 o posterior**.
- **Verificar el estado de actualización** desde la sección de *Configuración > Acerca del teléfono > Nivel de parche de seguridad*.
- **Evitar la instalación de aplicaciones fuera de Google Play**, dado que los entornos externos pueden incrementar la exposición a código malicioso.
- **Mantener habilitado Google Play Protect** para detectar y bloquear aplicaciones potencialmente dañinas.
- **Supervisar la disponibilidad de actualizaciones del fabricante**, especialmente en dispositivos que no reciben parches automáticos.
- **Establecer políticas de actualización periódica** en entornos corporativos que gestionen flotas de dispositivos Android.

En conclusión, esta vulnerabilidad refuerza la necesidad de **mantener los sistemas móviles actualizados** y de implementar prácticas continuas de seguridad preventiva, garantizando la protección frente a amenazas críticas de ejecución remota.

Fuente de Información:

- <https://gbhackers.com/android-hit-by-0-click-rce-vulnerability/>

	<b>ALERTA DE SEGURIDAD DIGITAL N°741</b>		<b>Fecha: 04-11-2025</b>
			<b>Página: 6 de 8</b>
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad crítica en el sistema Radiometrics VizAir.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Radiometrics Corporation ha publicado una vulnerabilidad de severidad <b>CRÍTICA</b> clasificada como CWE-522: Credenciales insuficientemente protegidas en el sistema Radiometrics VizAir, en la configuración de su API REST, que expone la clave del sistema en un archivo de configuración de acceso público. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado el acceso remoto no autorizado al sistema de monitoreo meteorológico.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>crítica</b> identificada por MITRE como <a href="#">CVE-2025-54863</a> de tipo credenciales insuficientemente protegidas en la configuración de su API REST, que expone la clave del sistema en un archivo de configuración de acceso público, podría permitir a un atacante alterar de forma remota los datos y configuraciones meteorológicas, automatizar ataques contra múltiples instancias y extraer datos meteorológicos confidenciales, lo que podría comprometer las operaciones aeroportuarias.</p> <p>Además, los atacantes podrían inundar el sistema con alertas falsas, lo que provocaría una denegación de servicio y una interrupción significativa de las operaciones aeroportuarias.</p> <p>El control remoto no autorizado de la monitorización meteorológica aeronáutica y la manipulación de datos podría dar lugar a una planificación de vuelo incorrecta y a condiciones peligrosas de despegue y aterrizaje.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>VizAir de Radiometrics Corporation (producto de monitorización/medición atmosférica), versiones anteriores a 08/2025.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>Actualizar inmediatamente el software VizAir a la versión parcheada que publica Radiometrics.</li> <li>Si una actualización no es inmediatamente posible, aislar el dispositivo/software de la red pública o restringir su acceso desde la red.</li> <li>Monitorear logs de acceso y comportamiento inusual en los sistemas VizAir, ya que una explotación remota puede dejar trazas de comandos o conexiones inesperadas.</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li><a href="https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-04">https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-04</a></li> </ul>	

	<b>ALERTA DE SEGURIDAD DIGITAL N°742</b>		Fecha: 04-11-2025
			Página: 7 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad en el software CNCSoft-G2 de Delta Electronics.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Delta Electronics ha publicado una vulnerabilidad de severidad <b>ALTA</b> clasificada como CWE-121: Desbordamiento de búfer basado en pila que afecta al software de control/edición para controladores CNCSoft-G2. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el contexto del proceso actual.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>alta</b> identificada por MITRE como <a href="#">CVE-2025-58317</a> de tipo desbordamiento de búfer basado en pila que afecta al software de control/edición para controladores CNCSoft-G2, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el contexto del proceso actual.</p> <p>Delta Electronics CNCSoft-G2 carece de la validación adecuada del archivo proporcionado por el usuario. Si un usuario abre un archivo malicioso, un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.</p> <p><b>A. Productos afectados:</b></p> <p>CNCSoft-G2: Versión 2.1.0.27 y anteriores.</p> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>Delta Electronics recomienda a los usuarios de CNCSoft-G2 que descarguen y actualicen a la versión 2.1.0.34 o posterior.</li> <li>No hacer clic en enlaces de Internet no confiables ni abra archivos adjuntos no solicitados en correos electrónicos.</li> <li>Evitar exponer los sistemas y equipos de control a Internet.</li> <li>Colocar los sistemas y dispositivos detrás de un firewall y aíslalos de la red empresarial.</li> <li>Cuando se requiera acceso remoto, utilizar un método de acceso seguro, como una red privada virtual (VPN).</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li><a href="https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-03">https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-03</a></li> </ul>	

## Índice alfabético

Troyanos ..... 4

Explotación de vulnerabilidades conocidas ..... 6,7