

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 de seguridad en WhatsApp permite la ejecución de URL maliciosas a través de Instagram Reels. 4

Índice alfabético 6

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°063		Fecha: 01-05-2026
			Página: 4 de 6
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Una vulnerabilidad de seguridad en WhatsApp permite la ejecución de URL maliciosas a través de Instagram Reels.		
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:

WhatsApp, plataforma de mensajería ampliamente utilizada a nivel global, fue objeto de una alerta de seguridad tras la identificación de dos vulnerabilidades relevantes corregidas por Meta en mayo de 2026. Estas fallas revelan riesgos asociados al procesamiento de contenidos enriquecidos y archivos adjuntos, particularmente cuando existen integraciones entre plataformas del mismo ecosistema digital, como WhatsApp e Instagram. Aunque no se ha confirmado explotación activa, el impacto potencial motivó la emisión inmediata de parches de seguridad por parte del fabricante.



Ilustración 1 Una vulnerabilidad de seguridad en WhatsApp permite la ejecución de URL maliciosas a través de Instagram Reels.

2. DETALLES:

La vulnerabilidad más crítica, identificada como CVE-2026-23866, se origina en una validación incompleta de mensajes enriquecidos que contienen vistas previas de Instagram Reels. Un atacante podría enviar un mensaje especialmente diseñado que fuerce a WhatsApp a procesar contenido multimedia desde una URL arbitraria y maliciosa. Este comportamiento permitiría activar manejadores de esquemas de URL del sistema operativo, abriendo aplicaciones externas o ejecutando acciones no autorizadas en el dispositivo de la víctima. La falla afecta versiones específicas de WhatsApp en Android e iOS.

Adicionalmente, se corrigió la vulnerabilidad CVE-2026-23863 en WhatsApp para Windows, donde archivos maliciosos podían disfrazarse mediante el uso de bytes NUL en el nombre del archivo, induciendo al usuario a ejecutar malware al abrir adjuntos aparentemente legítimos. Meta confirmó que ambas fallas fueron reportadas responsablemente y no existen evidencias de explotación en el entorno real hasta la fecha.

3. RECOMENDACIONES:

- Mantener WhatsApp y el sistema operativo siempre actualizados a las versiones más recientes disponibles.
- Desconfiar de enlaces o contenidos multimedia no solicitados, incluso si provienen de contactos conocidos.
- Evitar abrir archivos adjuntos en WhatsApp Desktop si no se ha verificado su origen y extensión real.
- Implementar soluciones de seguridad endpoint con detección de comportamiento (EDR/AV actualizado).
- Deshabilitar, cuando sea posible, la apertura automática de enlaces externos desde aplicaciones de mensajería.
- Capacitar a usuarios en conciencia de ciberseguridad, enfocándose en ataques por ingeniería social y archivos disfrazados.
- Revisar periódicamente los boletines de seguridad de Meta y aplicar parches de forma oportuna.

Fuente de Información:

- <https://gbhackers.com/whatsapp-security-flaw-enables-malicious-url-execution/>

Índice alfabético

Explotación de vulnerabilidades conocidas 4