



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

336-2026-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

El software espía GhostChat se dirige a los usuarios de Android a través de WhatsApp y roba datos confidenciales 4

Múltiples vulnerabilidades en WebSphere Application e IBM HTTP Server afectan a IBM Tivoli Monitoring. 6

Vulnerabilidad de ejecución remota de código en Delta Electronics DIAView. 7

Índice alfabético 8

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 336		Fecha: 29-01-2026
			Página: 4 de 8
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El software espía GhostChat se dirige a los usuarios de Android a través de WhatsApp y roba datos confidenciales		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Disponibilidad del Servicio		
Descripción			

1. ANTECEDENTES:

Investigadores de seguridad han identificado campañas activas donde los atacantes envían a la víctima un mensaje que aparenta venir de un contacto de confianza, normalmente con un gancho tipo “¿Eres tú en esta foto/video?”. Al hacer clic, la víctima es redirigida a una página que imita un visor de Facebook u otra red social y le pide “verificar” su cuenta antes de mostrar el contenido. El objetivo real es guiar paso a paso al usuario para que él mismo complete el flujo oficial de vinculación de dispositivos de WhatsApp, añadiendo silenciosamente el navegador del atacante como dispositivo enlazado.



Ilustración 1: GhostChat está dirigido a usuarios de WhatsApp (Fuente: welivesecurity)

2. DETALLES:

El flujo malicioso suele pedir primero el número de teléfono y luego mostrar un código de emparejamiento o un código QR, presentándolo como parte de una verificación de seguridad rutinaria.

La página, en realidad, inicia la función legítima de WhatsApp de “enlazar dispositivo por número/código” y retransmite a la víctima el mismo código que WhatsApp genera.

Cuando la víctima abre WhatsApp y, confiando en el mensaje, introduce el código o escanea el QR, autoriza sin saberlo el dispositivo del atacante, igual que si hubiera abierto WhatsApp Web en su propio PC.

Una vez vinculado, el atacante puede leer chats en tiempo real, ver histórico (según lo sincronizado), descargar fotos, videos y notas de voz, y escribir a contactos y grupos suplantando a la víctima.

El teléfono original sigue funcionando con normalidad, por lo que el usuario puede no notar nada salvo que revise la lista de “dispositivos vinculados”.


Con el control del chat, los atacantes pueden propagar la estafa reenviando el mismo gancho a otros contactos, ejecutar fraudes financieros, extorsión o recopilar más datos para futuras campañas.


3. RECOMENDACIONES:

- Desconfiar de enlaces recibidos por WhatsApp que prometen fotos/videos “comprometedores” o urgentes, incluso si parecen venir de un contacto conocido; confirmar por un canal alternativo antes de hacer clic.
- Nunca introducir tu número de teléfono ni códigos de verificación de WhatsApp en páginas web de terceros; los códigos sólo deben usarse dentro de la propia app cuando tú inicias el proceso.
- Revisar con frecuencia en WhatsApp: Ajustes → Dispositivos vinculados, y cerrar cualquier sesión/dispositivo que no reconozcas.
- Activar la verificación en dos pasos (PIN adicional) en WhatsApp para dificultar cambios de configuración de la cuenta.
- Formar a usuarios y personal sobre este patrón: páginas que imitan Facebook/otras redes y piden “verificar para ver la foto” suelen ser señuelo de toma de cuenta.
- En entorno corporativo, incluir WhatsApp (si se usa laboralmente) en la matriz de riesgos: políticas claras de uso, sensibilización frente a ingeniería social y procedimientos para reportar cuentas comprometidas y notificar a contactos afectados.

Fuente de Información:

- <https://gbhackers.com/ghostchat-targets-whatsapp-users/>

	ALERTA DE SEGURIDAD DIGITAL N°052		Fecha: 29-01-2026
			Página: 6 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en WebSphere Application e IBM HTTP Server afectan a IBM Tivoli Monitoring.		
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			
<p>1. ANTECEDENTES:</p> <p>IBM Corporation ha publicado dos vulnerabilidades de severidad MEDIA clasificadas como CWE-770: Asignación de recursos sin límites ni limitaciones y CWE-77: Inyección de comandos que afectan a IBM Tivoli Monitoring. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS) y ejecutar comandos SMTP arbitrarios en el sistema afectado.</p> <p>2. DETALLES:</p> <p>IBM Tivoli Monitoring es una solución de gestión y monitoreo de infraestructura de TI diseñada para supervisar en tiempo real el rendimiento, la disponibilidad y el estado de sistemas, servidores, aplicaciones y redes. Permite detectar de forma proactiva fallas, cuellos de botella y anomalías mediante métricas, alertas y paneles centralizados, ayudando a los equipos de TI a mantener la continuidad operativa, optimizar recursos y reducir tiempos de inactividad en entornos empresariales complejos y heterogéneos.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2025-36099 de tipo asignación de recursos sin límites ni limitaciones, podría permitir a un usuario remoto con privilegios realizar un ataque de denegación de servicio. La vulnerabilidad existe porque la aplicación no controla adecuadamente el consumo de recursos internos. Un usuario remoto con privilegios puede provocar el agotamiento de recursos y realizar un ataque de DoS.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2025-7962 de tipo inyección de comandos, podría permitir a un atacante remoto ejecutar comandos SMTP arbitrarios en el sistema. La vulnerabilidad existe debido a una validación de entrada insuficiente al manejar caracteres CR-LF en codificación UTF-8. Un atacante remoto puede pasar una entrada especialmente diseñada a la aplicación y ejecutar comandos SMTP arbitrarios en el servidor.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – IBM Tivoli Monitoring: 6.3.0 - 6.3.0.7 Service Pack 22. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. 			
Fuente de Información:	<ul style="list-style-type: none"> • hxxps://www.ibm.com/support/pages/node/7257410 • hxxps://www.ibm.com/support/pages/node/7246549 • hxxp://www.openwall.com/lists/oss-security/2025/09/03/4 • hxxps://gitlab.eclipse.org/security/cve-assignment/-/issues/67 		

	ALERTA DE SEGURIDAD DIGITAL N°053		Fecha: 29-01-2026
			Página: 7 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Delta Electronics DIAView.		
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			
<p>1. ANTECEDENTES:</p> <p>Delta Electronics, Inc. ha publicado una vulnerabilidad de severidad ALTA clasificada como CWE-749: Método o función peligrosa expuesta que afecta al software DIAView. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado la ejecución remota de código arbitrario en el sistema de destino.</p> <p>2. DETALLES:</p> <p>DIAView de Delta Electronics es un software de gestión y visualización industrial diseñado para supervisar, controlar y analizar datos de procesos en entornos de automatización. Permite integrar múltiples fuentes de datos de sistemas de control y sensores, presentar información en tiempo real mediante paneles gráficos y alertas, y facilitar la toma de decisiones operativas en industrias como manufactura, energía y servicios públicos.</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-0975 de tipo método o función peligrosa expuesta que afecta al software DIAView, podría permitir a un atacante no autenticado comprometer el sistema objetivo. La vulnerabilidad se debe a la exposición de una función peligrosa dentro del componente de script DIAView. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario en el sistema.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – DIAView: 4.2.0.0. <p>B. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – Ejecución de comandos inesperados en el sistema donde corre DIAView (por ejemplo: cmd.exe, powershell, sh, bash) invocados por el proceso de la aplicación. – Procesos hijos anómalos lanzados desde DIAView o servicios asociados (creación de shells, utilidades del sistema, scripts). – Archivos o scripts desconocidos creados recientemente en directorios temporales o de trabajo de la aplicación. – Cambios no autorizados en configuraciones del sistema o de DIAView sin intervención administrativa. – Registros (logs) con entradas malformadas o con caracteres especiales (; && \$() ``) en parámetros o campos de entrada. – Conexiones de red salientes inusuales desde el host industrial hacia IPs externas no habituales. – Incrementos anómalos de CPU/memoria del proceso DIAView coincidiendo con entradas de usuario o eventos de red. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. 			
Fuente de Información:		<ul style="list-style-type: none"> • https://www.zerodayinitiative.com/advisories/ZDI-26-049/ • https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00002_DIAView%20-Exposed%20Dangerous%20Method%20Remote%20Code%20Execution%20(CVE-2026-0975).pdf 	

Índice alfabético

Malware	4
Explotación de vulnerabilidades conocidas	6,7