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

007-2026-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 Aéreadel 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 lasempresas 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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°007	Fecha: 10-02-2026
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El phishing impulsado por IA y el fraude de códigos QR aumentan en 2025 según el informe sobre spam y phishing		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El informe reseñado expone que, durante 2025, el ecosistema de spam y phishing viró hacia campañas altamente personalizadas por IA generativa y un crecimiento marcado del quishing (uso de códigos QR en correos, PDFs y señalética física), mientras actores distribuyeron stealers e implants a escala aprovechando juegos/softwares crackeados y loaders por etapas. La IA se emplea para redactar señuelos coherentes y localizados, clonar estilos de marca y hasta simular asistentes de soporte conversacionales, lo que reduce señales clásicas de alerta y aumenta tasas de clic/respuesta; en paralelo, los QR desvían a portales de captura de credenciales, robo de MFA tokens o descargas maliciosas, a menudo desde dispositivos móviles menos monitorizados.

Ilustración 1: El phishing impulsado por IA y el fraude de códigos QR aumentan en 2025 según el informe sobre spam y phishing

2. DETALLES:

Los señuelos impulsados por IA permiten generar en minutos lotes de correos/mensajes con tono, gramática y branding realista, adaptando asuntos y contenido a perfil, geolocalización o coyuntura de noticias, lo que eleva la eficacia del BEC y de la suplantación de marcas. Chatbots/"asistentes" falsos guían paso a paso al usuario hasta introducir credenciales o pagos en formularios controlados por el atacante. En quishing, los adversarios insertan QR en correos, facturas PDF o cartelería, explotando el menor escrutinio de imágenes por pasarelas de correo y la lectura con móviles personales; al escanear, la víctima llega a portales de phishing, páginas para robo de MFA o sitios de descarga de malware (currier/SaaS/nómina simulados). Además, se observó una cadena de infección por etapas vinculada a software/juegos pirateados para desplegar HijackLoader/stealers (p. ej., Lumma, ACR), con desempaquetado y ejecución encubiertos mediante loaders modulares y técnicas de inyección en librerías del sistema, multiplicando el alcance y la persistencia.

3. RECOMENDACIONES:

- Filtrado avanzado de correo y análisis visual: combinar Secure Email Gateway con detección por visión computacional y análisis de contenidos para imágenes/QR, brand-impersonation y plantillas dinámicas generadas por IA.
- Políticas móviles y BYOD: reforzar MDM/MAM en dispositivos que escanean QR (navegación aislada, verificación de URLs, bloqueo de side-loading y protección contra stealers en Android/iOS).
- Autenticación y anti-spoofing: exigir MFA resistente a phishing (FIDO2/passkeys) y endurecer SPF, DKIM, DMARC con políticas de quarantine/reject y monitoreo de dominios look-alike.
- Aislamiento de navegación y sandbox de adjuntos: abrir enlaces y documentos externos en navegadores aislados/contenedores; bloquear redirecciones desde QR hacia dominios recién creados o sin reputación.
- Detección de loaders y respuesta: instrumentar reglas EDR/XDR para hilos por etapas (descifrado en memoria, inyección en DLL de sistema, comportamiento de hijack loaders), con contención automática y revocación de tokens ante sospecha.
- Concienciación continua y simulaciones: capacitar sobre señuelos generados por IA y QR maliciosos; realizar simulacros multicanal (correo/SMS/QR) y campañas de reporte temprano (report-phish) con métricas de clic/escalado

Fuente de Información:	• hxxps://gbhackers.com/spam-and-phishing-report/

	ALERTA DE SEGURIDAD DIGITAL N°071	Fecha: 10-02-2026
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en parámetros de comando de OpenClaw		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

OpenClaw ha publicado una vulnerabilidad de severidad **ALTA** clasificada como CWE-669: Transferencia incorrecta de recursos entre esferas que afecta a OpenClaw (también conocido como clawdbot o Moltbot). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante exfiltrar un tokens de autenticación mediante un enlace malicioso que manipula el parámetro gatewayUrl, forzando una conexión WebSocket automática sin confirmación del usuario que transmite las credenciales al servidor del atacante.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2026-25253 de tipo CWE-669: Transferencia incorrecta de recursos entre esferas que afecta a OpenClaw (también conocido como clawdbot o Moltbot), podría permitir a un atacante exfiltrar un tokens de autenticación mediante un enlace malicioso que manipula el parámetro gatewayUrl, forzando una conexión WebSocket automática sin confirmación del usuario que transmite las credenciales al servidor del atacante. Una vez obtenido el token, el atacante puede realizar secuestro de WebSocket entre sitios (CSWSH) para comprometer el gateway local y lograr ejecución remota de código (RCE) con un solo clic.

A. Productos afectados:

- OpenClaw (clawdbot o Moltbot) en versiones anteriores a 2026.1.29.

B. Indicadores de compromiso:

- Conexiones WebSocket no autorizadas a URLs de gateway maliciosas iniciadas automáticamente desde el navegador de la víctima,
- Exfiltración de tokens de autenticación en respuestas WebSocket, permitiendo acceso remoto al gateway local de la víctima incluso si está configurado solo en loopback,
- Actividad sospechosa como ejecución de comandos remotos o accesos no autorizados al gateway potencialmente visibles en logs de red o del navegador.

3. RECOMENDACIONES:

- Actualizar a OpenClaw versión 2026.1.29 o superior para corregir la validación automática de gatewayUrl,
- Implementar políticas de bloqueo de conexiones WebSocket salientes no confiables,
- Validar URLs de gateway manualmente y monitoree tokens sensibles en el tráfico de red,
- Evitar hacer clic en enlaces sospechosos. Para sistemas expuestos, revise logs en busca de IOCs y considere firewalls que restrinjan conexiones outbound a gateways no autorizados.

Fuente de Información:	• hxxps[:]//openclaw[.]ai/blog • hxxps[:]//ethiack[.]com/news/blog/one-click-rce-moltbot • hxxps[:]//github[.]com/openclaw/openclaw/security/advisories/GHSA-g8p2-7wf7-98mq

	ALERTA DE SEGURIDAD DIGITAL N°072	Fecha: 10-02-2026
		Página: 7 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Fortinet ha lanzado una actualización de seguridad que corrige una vulnerabilidad crítica que afecta a FortiClientEMS.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	**Abreviatura**	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	H	**Código de Sub familia**	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Fortinet, Inc. ha lanzado una actualización de seguridad que corrige una vulnerabilidad de severidad **CRÍTICA** clasificada como CWE-89: Ejecutar código o comandos no autorizados que afecta a Fortinet FortiClientEMS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código o comandos no autorizados mediante solicitudes HTTP específicamente diseñadas.

2. **DETALLES:**

FortiClient EMS es un servidor de gestión centralizada que permite a los administradores de seguridad controlar agentes FortiClient instalados en estaciones de trabajo y servidores.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2026-21643 de tipo CWE-89: Ejecutar código o comandos no autorizados que afecta a Fortinet FortiClientEMS, podría permitir a un atacante remoto no autenticado ejecutar código o comandos no autorizados mediante solicitudes HTTP específicamente diseñadas.

Una neutralización incorrecta de elementos especiales usados en una vulnerabilidad de comandos sql (inyección sql) en Fortinet FortiClientEMS 7.4.4 puede permitir que un atacante no autenticado ejecute código o comandos no autorizados mediante solicitudes HTTP específicamente diseñadas.

A. Productos afectados:

- FortiClientEMS 7.4.4 (Actualización a 7.4.5 o superior).

3. **RECOMENDACIONES:**

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://fortiguard.fortinet.com/psirt/FG-IR-25-1142

Índice alfabético