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

010-2026-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°010	Fecha: 13-02-2026
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El exploit ZeroDayRAT ataca Android e iOS, lo que permite la vigilancia en tiempo real y el robo masivo de datos.		
Tipo de Ataque	Exploits	Abreviatura	Exploits
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Investigadores han documentado la aparición de ZeroDayRAT, una plataforma comercial de spyware para móviles que se vende abiertamente en canales de Telegram desde el 2 de febrero de 2026. Permite a atacantes tomar control remoto completo de Android 5–16 y iOS hasta 26, con panel web para gestionar víctimas, y se propaga principalmente mediante smishing, apps falsas y mercados no oficiales. La operación incluye canales de ventas, soporte y actualizaciones, rebajando la barrera técnica para ejecutar vigilancia en tiempo real y robo de datos/finanzas.

Ilustración 1: El exploit ZeroDayRAT ataca Android e iOS, lo que permite la vigilancia en tiempo real y el robo masivo de datos.

2. DETALLES:

ZeroDayRAT ofrece a los operadores un panel auto-alojado que perfila el dispositivo (modelo, OS, operador/SIM, batería), muestra historial de actividad, uso de apps y previsualiza SMS, facilitando ingeniería social y TTPs de account takeover, Incluye pestañas para ubicación GPS en tiempo real y histórico (Google Maps embebido), y captura notificaciones de WhatsApp, Instagram, banca y sistema sin abrir apps, otorgando visibilidad pasiva de casi toda la actividad, Integra intercepción de SMS y OTP, lo que debilita el 2FA por SMS; además habilita streaming de cámara/micrófono, grabación de pantalla y keylogging con vista en vivo, convirtiendo el teléfono en un dispositivo de vigilancia.

Para monetización, aporta módulos de robo financiero: crypto stealer (detección de wallets y clipboard injection para redirigir transacciones) y bank stealer con overlays sobre apps bancarias y pagos (incl. Google Pay/Apple Pay/UPI).

El modelo de distribución descentralizado (cada actor aloja su infraestructura) complica la interrupción/takedown y acelera la proliferación entre ciberdelincuentes sin alta pericia.

3. RECOMENDACIONES:

- Migrar de 2FA por SMS a MFA resistente al phishing (llaves FIDO2/WebAuthn o passkeys) para neutralizar interceptación de OTP.
- No instalar apps fuera de tiendas oficiales y deshabilitar “orígenes desconocidos” en Android; en iOS, evitar perfiles no corporativos y verificar la procedencia de apps.
- Mantener sistemas y apps actualizados (parches de seguridad al día) para reducir superficie de explotación en móviles.
- Endurecer permisos: revisar y revocar Accesibilidad, Superposición, Administración del dispositivo, Cámara/Micrófono y Ubicación en apps no esenciales.
- Usar soluciones MTD/EDR móvil integradas con MDM para detectar overlays, abuso de accesibilidad, keylogging y exfiltración; aplicar políticas de protección de apps (contenedorización de datos).
- Higiene de notificaciones: ocultar contenido sensible en pantalla bloqueada (especialmente banca y OTP) para limitar la recolección pasiva.
- Concienciación anti-smishing: formar a usuarios para no abrir enlaces ni instalar “actualizaciones” desde SMS o mensajería; verificar remitentes y dominios.
- Uso de VPN y DNS filtrado en movilidad (cuando aplique) para bloquear dominios maliciosos y endurecer navegación en redes no confiables.
- Protección financiera: verificar manualmente direcciones antes de transferencias cripto (evita clipboard hijacking) y activar alertas fuera de banda para transacciones.
- Plan de respuesta en móviles: ante sospecha, aislar el equipo (modo avión + Wi-Fi/Bluetooth off), preservar evidencias, revocar tokens/sesiones, rotar contraseñas y restaurar de fábrica antes de re-inscribir en MDM.

Fuente de Información:	• https://gbhackers.com/zerodayrat-exploit-targets-android-ios/

	ALERTA DE SEGURIDAD DIGITAL N°077	Fecha: 13-02-2026
		Página: 6 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en productos Cisco.		
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:**

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** clasificada como CWE-94: Control inadecuado de la generación de código (Inyección de código) que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.

2. **DETALLES:**

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2026-20045 de tipo CWE-94: Inyección de código en Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unity Connection y Cisco Webex Calling Dedicated Instance, podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.

Esta vulnerabilidad se debe a una validación incorrecta de la información proporcionada por el usuario en las solicitudes HTTP. Un atacante podría explotar esta vulnerabilidad enviando una secuencia de solicitudes HTTP manipuladas a la interfaz de administración web de un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener acceso de usuario al sistema operativo subyacente y, posteriormente, elevar los privilegios a root.

Cisco ha asignado a este aviso de seguridad una Clasificación de Impacto de Seguridad (SIR) Crítica, en lugar de Alta, como indica la puntuación. Esto se debe a que la explotación de esta vulnerabilidad podría provocar que un atacante eleve los privilegios a root.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco, independientemente de la configuración del dispositivo:

- CM unificado,
- CM SME unificado,
- CM IM&P unificado,
- Conexión de Unity,
- Instancia dedicada de Webex Calling.

3. **RECOMENDACIONES:**

- Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas. Cisco considera que las soluciones alternativas y mitigaciones (si procede) son temporales hasta que esté disponible una actualización a una versión de software corregida. Para remediar completamente esta vulnerabilidad y evitar futuras exposiciones, como se describe en este aviso, Cisco recomienda encarecidamente a los clientes que actualicen al software corregido indicado en este aviso.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

	ALERTA DE SEGURIDAD DIGITAL N°078	Fecha: 13-02-2026
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Exploit para control de acceso indebido en Web Help Desk.		
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:

SolarWinds ha publicado una vulnerabilidad de severidad **ALTA** clasificada como CWE-284: Control de acceso inadecuado que afecta a Web Help Desk (WHD). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a una funcionalidad que de otro modo estaría restringida.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-40536 de tipo CWE-284: Control de acceso inadecuado que afecta a SolarWinds Web Help Desk, podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a una funcionalidad que de otro modo estaría restringida.

La vulnerabilidad existe debido a restricciones de acceso indebidas. Un atacante remoto no autenticado puede eludir las restricciones de seguridad implementadas y, en determinadas circunstancias, obtener acceso no autorizado a la aplicación, lo que podría comprometerla.

A. Productos afectados:

- Web Help Desk.

3. RECOMENDACIONES:

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

Fuente de Información:	• hxxps://www.cybersecurity-help.cz/vdb/exploit/12414/ • hxxps://www.rapid7.com/db/modules/exploit/multi/http/solarwinds_webhelpdesk_rce

Índice alfabético