



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

043-2026-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

Un malware respaldado por GitHub se propaga a través de archivos LNK en Corea del Sur 4

Vulnerabilidad crítica en mbCONNECT24 permite la inyección sql remota sin autenticación. 6

Índice alfabético 7

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°043		Fecha: 01-04-2026
			Página: 4 de 7
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Un malware respaldado por GitHub se propaga a través de archivos LNK en Corea del Sur		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		
Descripción			

1. ANTECEDENTES:

En los últimos años, actores de amenazas avanzadas han incrementado el abuso de plataformas legítimas y ampliamente confiables para evadir controles de seguridad tradicionales. GitHub, por su reputación y uso extendido en entornos corporativos y de desarrollo, se ha convertido en un vector atractivo para alojar y distribuir código malicioso sin levantar sospechas inmediatas. Esta tendencia refleja una evolución clara hacia técnicas "living-off-the-land", donde los atacantes se mezclan con el tráfico normal y aprovechan la confianza implícita en servicios en la nube para mantener persistencia y sigilo operativo.



Ilustración 1 Los piratas informáticos están abusando de los archivos de acceso directo de Windows y de GitHub

2. DETALLES:

La alerta publicada por GBHackers describe una campaña en la que atacantes respaldados por un grupo APT vinculado a Corea del Norte (Kimsuky) utilizan repositorios de GitHub como infraestructura para distribuir y controlar malware. El ataque inicia con archivos ZIP que contienen accesos directos maliciosos (.LNK) disfrazados de documentos legítimos, como facturas electrónicas en formato PDF. Al ejecutar el archivo, se activa un comando oculto de PowerShell que descarga cargas útiles adicionales desde repositorios controlados por los atacantes en GitHub.


El malware implementa un mecanismo de persistencia mediante tareas programadas que se ejecutan periódicamente, simulando procesos del sistema, y recopila información sensible del equipo comprometido (datos del sistema, red y procesos activos), la cual es exfiltrada nuevamente a GitHub utilizando tokens de acceso embebidos en los scripts. Este enfoque dificulta la detección, ya que el tráfico se camufla como actividad legítima hacia un dominio ampliamente permitido en organizaciones.

3 RECOMENDACIONES:

- Restringir y monitorear de forma avanzada el tráfico hacia api.github.com y repositorios GitHub, aplicando análisis de comportamiento y no solo listas de permitidos.
- Habilitar registro y auditoría extendida de PowerShell (Script Block Logging y AMSI) en todos los endpoints corporativos.
- Implementar detección de creación de tareas programadas sospechosas, especialmente aquellas con nombres que imitan componentes del sistema.
- Bloquear o filtrar la ejecución de archivos .LNK provenientes de correos electrónicos o descargas externas.
- Aplicar Zero Trust para scripts y binarios descargados desde servicios en la nube, aun cuando sean legítimos.
- Fortalecer la concienciación del usuario sobre archivos adjuntos disfrazados de documentos comunes y campañas de ingeniería social.
- Mantener soluciones EDR/XDR actualizadas con capacidad de detección de ataques multietapa y abuso de servicios legítimos.

Fuente de Información:

- <https://gbhackers.com/github-backed-malware/>

	ALERTA DE SEGURIDAD DIGITAL N°181		Fecha: 01-04-2026
			Página: 6 de 7
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en mbCONNECT24 permite la inyección sql remota sin autenticación.		
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			
<p>1. ANTECEDENTES:</p> <p>MB connect line ha reportado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-89: Inyección SQL que afecta a mbCONNECT24, la cual permite a un atacante remoto no autenticado manipular consultas a la base de datos, comprometiendo la integridad y disponibilidad del sistema, con potencial impacto en la gestión remota de infraestructuras industriales.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-33615 reside en el endpoint setinfo, donde las entradas proporcionadas por el usuario no son correctamente validadas ni sanitizadas antes de ser utilizadas en una sentencia SQL de tipo UPDATE. Esto permite que un atacante inserte código SQL arbitrario dentro de la consulta, alterando su lógica original y ejecutando comandos no previstos por el sistema.</p> <p>El fallo se produce debido a la falta de uso de consultas parametrizadas o mecanismos de escape adecuados, lo que habilita ataques clásicos de SQL Injection como manipulación de condiciones (OR 1=1), concatenación de consultas o modificación directa de registros. Dado que el servicio es accesible por red y no requiere autenticación, la explotación puede realizarse de forma remota con baja complejidad.</p> <p>La explotación de esta vulnerabilidad puede derivar en la modificación arbitraria de datos críticos, eliminación de registros o corrupción de la base de datos, afectando directamente la operación del sistema. En entornos industriales, esto puede traducirse en interrupciones operativas, pérdida de control de dispositivos remotos y posibles impactos en procesos físicos.</p> <p>Hasta el momento, no existe evidencia pública confirmada de explotación activa por parte de actores de amenaza; sin embargo, debido a la criticidad y simplicidad del exploit, es altamente probable su adopción en campañas maliciosas. Asimismo, ya se han identificado vectores de prueba y demostraciones técnicas (PoC) que permiten validar la vulnerabilidad, lo que incrementa significativamente el riesgo de explotación en entornos expuestos.</p> <p>El riesgo es crítico, especialmente para organizaciones que utilizan mbCONNECT24 en entornos OT/ICS expuestos a Internet. La combinación de acceso remoto, ausencia de autenticación y facilidad de explotación convierte esta vulnerabilidad en un vector ideal para ataques disruptivos, sabotaje o preparación de accesos persistentes en la infraestructura.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – mbCONNECT24 ≤ versión 2.19.4. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software disponible que corrige esta vulnerabilidad. • Implementar validación estricta de entradas (input validation). • Uso obligatorio de consultas parametrizadas (prepared statements). • Restringir el acceso al servicio mediante VPN o listas blancas. • Implementar WAF con reglas específicas para SQL Injection. • Monitorear logs y eventos relacionados con consultas SQL. 			
Fuente de Información:		<ul style="list-style-type: none"> • https://certvde.com/de/advisories/VDE-2026-030 • https://mbconnectline.csaf-tf.certvde.com/.well-known/csaf/white/2026/vde-2026-030.json 	

Índice alfabético

Malware 4

Explotación de vulnerabilidades conocidas 6