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

128-2025-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°128	Fecha: 03-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El troyano Crocodilus para Android se expandió a nivel mundial con nuevas funciones cripto y de robo bancario		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Un número creciente de campañas maliciosas han aprovechado un troyano bancario para Android recientemente descubierto llamado Crocodilus para atacar a usuarios de Europa y Sudamérica.

Crocodilus se documentó públicamente por primera vez en marzo de 2025, atacando a usuarios de dispositivos Android en España y Turquía haciéndose pasar por aplicaciones legítimas como Google Chrome.

2. DETALLES:

El malware, según un nuevo informe publicado por ThreatFabric, también ha adoptado técnicas de ofuscación mejoradas para dificultar el análisis y la detección, e incluye la capacidad de crear nuevos contactos en la lista de contactos de la víctima, lo que permite a los atacantes insertar números de teléfono etiquetados como "Soporte bancario", que podrían utilizarse para ataques de ingeniería social.

Cuenta también con la capacidad de lanzar ataques de superposición contra una lista de aplicaciones financieras obtenidas de un servidor externo para recopilar credenciales.

También abusa de los permisos de los servicios de accesibilidad para capturar frases semilla asociadas a billeteras de criptomonedas, que luego pueden usarse para drenar los activos virtuales almacenados en ellas.

La última variante del troyano cuenta con código empaquetado, cifrado XOR adicional y una lógica intencionadamente enrevesada para resistir la ingeniería inversa.

Crocodilus se centra en aplicaciones bancarias y de criptomonedas. Una vez instalado, superpone páginas de inicio de sesión falsas sobre aplicaciones bancarias y cripto legítimas. En España, se hizo pasar por una actualización del navegador y atacó a casi todos los principales bancos.

En otros casos, utilizan anuncios falsos en Facebook como vector de distribución, imitando a bancos y plataformas de comercio electrónico. Estos anuncios incitan a las víctimas a descargar una aplicación para obtener supuestos puntos de bonificación. Los usuarios que intentan descargar la aplicación son redirigidos a un sitio malicioso que distribuye el dropper Crocodilus.

3. RECOMENDACIONES:

- Evitar instalar aplicaciones de fuentes no verificadas.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Implementar sistemas avanzados de análisis de comportamiento y evaluación de riesgos en tiempo real para detectar posibles fraudes antes de que se materialicen
- Promover la cooperación global en el intercambio de información sobre amenazas, el desarrollo de marcos regulatorios y el fortalecimiento de capacidades de respuesta ante incidentes.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing

Fuente de Información:	• hxxps://thehackernews.com/2025/06/android-trojan-crocodilus-now-active-in.html • hxxps://es.tradingview.com/news/cointelegraph:95d72147009cd:0/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°128	Fecha: 03-06-2025
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el servidor VPN Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series Teleworker Gateway		
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:

Cisco Systems ha publicado una vulnerabilidad de severidad **MEDIA** de tipo condición de carrera que afecta al servidor VPN Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series Teleworker Gateway. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado secuestrar una sesión VPN AnyConnect o provocar una condición de denegación de servicio (DoS) para usuarios individuales del servicio VPN AnyConnect en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-20509 de tipo condición de carrera que afecta al servidor VPN Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series Teleworker Gateway, podría permitir a un atacante remoto no autenticado secuestrar una sesión VPN AnyConnect o provocar una condición de denegación de servicio (DoS) para usuarios individuales del servicio VPN AnyConnect en un dispositivo afectado.

Esta vulnerabilidad se debe a una entropía débil para los controladores utilizados durante el proceso de autenticación de VPN, así como a una condición de carrera presente en dicho proceso. Un atacante podría explotar esta vulnerabilidad adivinando correctamente un controlador de autenticación y enviando solicitudes HTTPS manipuladas a un dispositivo afectado. Una explotación exitosa podría permitir al atacante tomar el control de la sesión VPN de AnyConnect de un usuario objetivo o impedir que este establezca una sesión VPN de AnyConnect con el dispositivo afectado.

A. Productos afectados:

- Al momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos Cisco Meraki si ejecutaban una versión vulnerable del firmware Cisco Meraki MX y tenían Cisco AnyConnect VPN habilitado: MX64, MX64W, MX65, MX65W, MX67, MX67C, MX67W, MX68, MX68CW, MX68W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600, vMX, Z3, Z3C, Z4, Z4C.

Nota: Cisco AnyConnect VPN es compatible con los dispositivos Cisco Meraki MX Series y Cisco Meraki Z Series Teleworker Gateway que ejecutan versiones de firmware de Cisco Meraki MX 16.2 y posteriores, excepto Cisco Meraki MX64 y MX65, que son compatibles con Cisco AnyConnect VPN solo si ejecutan versiones de firmware de Cisco Meraki MX 17.6 y posteriores.

3. RECOMENDACIÓN:

- Actualizar la versión según la última publicación de Cisco Meraki para solucionar esta vulnerabilidad. No existen soluciones alternativas que la solucionen. Sin embargo, deshabilitar Cisco AnyConnect VPN eliminará el vector de ataque para la vulnerabilidad que se describe en este aviso.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°128	Fecha: 03-06-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de severidad crítica en Google Chrome		
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:

Se ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo escritura fuera de límites y uso posterior a la liberación que afecta a Google Chrome. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo y obtener acceso a información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5419 de tipo escritura fuera de límites, podría permitir a un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a un error de límite en el motor V8. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado, activar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-5068 de tipo uso posterior a la liberación, podría permitir un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a un error de uso tras liberación en Blink en Google Chrome. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, generar un error de uso tras liberación y obtener acceso a información confidencial.

A. Productos afectados:

- Google Chrome: 100.0.4896.60 - 137.0.7151.56.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html • hxxps://crbug.com/409059706 • hxxps://crbug.com/420636529

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°128	Fecha: 03-06-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en equipos MELSEC iQ-F Series de Mitsubishi Electric		
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:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo validación incorrecta del índice, la posición o el desplazamiento especificados en la entrada que afecta a equipos MELSEC iQ-F Series de Mitsubishi Electric. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado leer información confidencial, provocar una condición de denegación de servicio o detener operaciones mediante el envío de paquetes especialmente diseñados.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3755 de tipo validación incorrecta del índice, la posición o el desplazamiento especificados en la entrada que afecta a equipos MELSEC iQ-F Series de Mitsubishi Electric, podría permitir a un atacante remoto no autenticado leer información confidencial, provocar una condición de denegación de servicio o detener operaciones mediante el envío de paquetes especialmente diseñados.

Esta vulnerabilidad permite a un atacante remoto leer información del producto, provocar una denegación de servicio (DoS) en la comunicación de conexión de MELSOFT con productos Mitsubishi Electric FA como GX Works3 y GOT, o detener el funcionamiento del módulo de CPU (lo que provoca una DoS en el módulo de CPU) mediante el envío de paquetes especialmente diseñados. Es necesario reiniciar el producto para la recuperación.

A. Productos afectados:

- FX5U-xMy/zx=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS: todas las versiones.
- FX5UC-xMy/zx=32, 64, 96, y=T, z=D, DSS: Todas las versiones.
- FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS: todas las versiones.
- FX5UJ-xMy/zx=24, 40, 60, y=T, R, z=ES, DS, ESS, DSS: todas las versiones.
- FX5UJ-xMy/ES-A[Nota *1] x=24, 40, 60, y=T, R: Todas las versiones.
- FX5S-xMy/zx=30, 40, 60, 80[Nota *1], y=T, R, z= ES, DS, ESS, DSS: todas las versiones.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Utilizar un firewall o una red privada virtual (VPN), etc. para evitar el acceso no autorizado cuando se requiera acceso a Internet.
- Usar los equipos dentro de una LAN y bloquear el acceso desde redes y hosts no confiables a través de firewalls.
- Utilizar la función de filtro IP para bloquear el acceso desde hosts que no sean de confianza.
- Restringir el acceso físico a los productos afectados y a la LAN a la que están conectados.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-153-03 • hxxps://www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-003_en.pdf • hxxps://www.mitsubishielectric.com/fa/download/index.html

Índice alfabético