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

127-2025-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°127	Fecha: 02-06-2025 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Cibercriminales suplantan sitio de CapCut para difundir malware		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

ESET alerta sobre un nuevo engaño en el que crean sitios falsos cuya URL presenta variaciones imperceptibles con respecto al oficial y que a simple vista parecen legítimos. En este caso con el objetivo de distribuir un falso instalador que infecta con malware en el equipo que lo descargue.

2. DETALLES:

Un sitio web falso que imita al dominio oficial de CapCut, una popular aplicación de edición de videos, ha sido identificado como un medio para distribuir malware. Según un análisis de ESET, el software malicioso, detectado como JS/Kryptik.CWH, se propaga a través de una página web cuya dirección URL presenta una variación casi imperceptible respecto al sitio legítimo.

El dominio oficial de CapCut es www[.]capcut[.]com, mientras que el sitio fraudulento añade una letra “i” al final de la palabra “cut”, resultando en www[.]capcuti[.]com. Esta sutil diferencia puede pasar desapercibida para los usuarios, especialmente aquellos que buscan la aplicación en motores de búsqueda como Google. Según ESET, es probable que este sitio falso haya sido promovido mediante anuncios en los resultados de búsqueda o en redes sociales, estrategias que ya se han utilizado anteriormente para engañar a los usuarios. Por otro lado, si se trata de una app para dispositivos móviles, es más fácil caer en la trampa para quienes no presten la debida atención.

El supuesto instalador de CapCut, que se descarga al hacer clic en el botón “Download for Windows” es un archivo comprimido en formato .zip que contiene un ejecutable con nombre Installer-<NUMERO_INSTALACION>.exe y una carpeta llamada AppData. Este archivo ejecutable se trata de un instalador NSIS que contiene un script que se utiliza para instalar y ejecutar archivos en la máquina de la víctima.

Este script invoca a un archivo de configuración .ini, el cual se encuentra dentro de la ruta AppData\AppInfo\Launcher incluido en el archivo comprimido mencionado previamente. Este archivo va a ejecutar un programa llamado Installer.<NUMERO_INSTALACION>.exe pasándole por argumento dos datos, por un lado, una DLL llamada Installer-<NUMERO_INSTALACION> y, por otro lado, un número hardcodeado 2175608479.

El archivo a ejecutar en cuestión posee el hash BFD37182CD581BE0F605FEA0E15D5FD39FD3D1BE, y se trata del binario oficial de node JS que permite ejecutar código JavaScript en una máquina. Sin embargo, la DLL que le pasa como argumento es en realidad un código javascript con varias capas de ofuscación detectado por las tecnologías de ESET como JS/Kryptik.CWH.

Lo que busca es ejecutar código malicioso dentro de la máquina de la víctima que puede derivar en el robo de credenciales de acceso a cuentas, entre muchas otras acciones maliciosas posibles.

3. RECOMENDACIONES:

- No confiar ciegamente en los primeros resultados de Google o en sitios a los que llegamos por anuncios en redes sociales.
- Analizar la URL del sitio y hacer una segunda búsqueda ante la duda.
- Instalar un software antimalware en los dispositivos para identificar y bloquear sitios web falsos, incluso detectar y detener la ejecución de archivos maliciosos, ya sea en computadoras o teléfonos móviles.

Fuente de Información:	• hxxps://www.welivesecurity.com/es/estafas-enganos/aplicacion-falsa-capcut-instala-malware/ • hxxps://www.infobae.com/tecno/2025/05/27/suplantan-a-la-famosa-aplicacion-de-edicion-de-video-capcut-instala-malware-y-roba-datos/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 02-06-2025 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software HPE StoreOnce		
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 autenticación incorrecta en el software HPE StoreOnce. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado el acceso no autorizado al sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-37093 de tipo omisión de autenticación que afecta al software HPE StoreOnce, podría permitir a un atacante obtener acceso no autorizado a los sistemas que ejecutan el software vulnerable, lo que podría comprometer la confidencialidad, la integridad y la disponibilidad de los datos almacenados.

La explotación exitosa permite a un atacante eludir los mecanismos de autenticación, lo que le otorga acceso no autorizado con privilegios potencialmente completos. Los atacantes podrían acceder a datos confidenciales, modificar configuraciones del sistema o interrumpir operaciones de respaldo y recuperación, lo que provocaría violaciones de datos o interrupciones del servicio. La vulnerabilidad puede ser explotada de forma remota, sin necesidad de interacción del usuario o autenticación previa.

Esta vulnerabilidad supone un riesgo significativo para las organizaciones que dependen de HPE StoreOnce para la protección de datos. Se recomienda estar al tanto y prepararse de inmediato para su solución.

No se han reportado exploits de prueba de concepto (PoC) ni intentos de explotación activa.

A. Productos afectados:

- Software HPE StoreOnce, versión 4.3.11 o posterior.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software cuando esté disponible. HPE aún no ha proporcionado una actualización de seguridad ni una guía de mitigación.
- Monitorear las actualizaciones oficiales de HPE StoreOnce y aplicar parches de seguridad tan pronto como estén disponibles.
- Restringir el acceso de red a las interfaces de administración de HPE StoreOnce siempre que sea posible.
- Supervisar los registros para detectar patrones de acceso o autenticación inusuales.

Fuente de Información:	• hxxps://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04847en_us&docLocale=en_US

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 02-06-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el controlador del punto de acceso WLAN de MediaTek		
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:

MediaTek, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización incorrecta en el controlador del punto de acceso WLAN, causada por la falta de una comprobación de permisos que permite la inyección remota de paquetes arbitrarios. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la escalada de privilegios mediante la inyección de paquetes arbitrarios.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20674 de tipo autorización incorrecta en el controlador del punto de acceso WLAN, podría permitir a un atacante remoto no autenticado la inyección de paquetes arbitrarios. Un atacante podría explotar esta vulnerabilidad para escalar privilegios remotamente sin necesidad de privilegios de ejecución adicionales ni interacción del usuario. Esto supone un riesgo significativo para la seguridad de la red, ya que podría permitir el acceso y control no autorizados del punto de acceso inalámbrico.

La vulnerabilidad en el controlador del punto de acceso WLAN, existe debido a una forma posible de inyectar un paquete arbitrario por la falta de verificación de permisos. Esto podría provocar una escalada remota de privilegios sin necesidad de privilegios de ejecución adicionales.

Esta vulnerabilidad forma parte de un conjunto más amplio de problemas revelados por MediaTek en junio de 2025 que afectan a los subsistemas WLAN, Bluetooth e IMS. La vulnerabilidad CVE-2025-20674 destaca porque permite a atacantes remotos inyectar paquetes arbitrarios aprovechando la falta de verificación de permisos en el controlador del punto de acceso WLAN, lo que podría provocar una escalada de privilegios no autorizada sin interacción del usuario.

A. Productos afectados:

- Controlador del punto de acceso WLAN en chipsets MediaTek.
- Chipsets afectados: MT6890, MT6990, MT7915, MT7916, MT7981, MT7986, MT7990, MT7992, MT7993, todas las versiones.
- Versiones de software afectadas: Versión del SDK 7.6.7.2 y anteriores / OpenWrt 19.07, 21.02 (MT6890) / OpenWrt 21.02, 23.05 (MT6990).

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Realizar una revisión exhaustiva de las configuraciones de los puntos de acceso inalámbricos.
- Implementar una segmentación estricta de la red.
- Monitorear el tráfico de la red para detectar intentos sospechosos de inyección de paquetes.
- Verificar y aplicar los mecanismos de autorización adecuados en la infraestructura de la red inalámbrica.

Fuente de Información:	• hxxps://corp.mediatek.com/product-security-bulletin/June-2025

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°127	Fecha: 02-06-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en procesadores Exynos 1480 y Exynos 2400 de Samsung		
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:

Samsung ha publicado una vulnerabilidad de severidad **ALTA** de tipo Escritura fuera de límites en los procesadores para móvil Exynos 1480 y Exynos 2400. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-23107 de tipo escritura fuera de límites en los procesadores para móvil Exynos 1480 y Exynos 2400. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad existe debido a un error de límite al procesar entradas no confiables. Un atacante remoto puede activar una escritura fuera de los límites y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Exynos 1480: Todas las versiones.
- Exynos 2400: Todas las versiones.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://semiconductor.samsung.com/content/semiconductor/global/support/quality-support/product-security-updates/cve-2025-23107/

Índice alfabético