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

228-2024-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°228	Fecha: 02-10-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos de FIN7 lanzan sitios generadores de desnudos deepfake para difundir malware		
Tipo de Ataque	Stealers	Abreviatur	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El famoso grupo de piratería APT conocido como FIN7 ha lanzado una red de sitios falsos generadores de deepnude impulsados por IA para infectar a los visitantes con malware que roba información.

Esta intrincada red de sitios web promueven generadores de desnudos profundos que afirman crear versiones falsas de desnudos de fotos de individuos vestidos. La tecnología ha sido controvertida debido al daño que puede causar a los sujetos al crear imágenes explícitas no consentidas, e incluso ha sido prohibida en muchos lugares del mundo. Sin embargo, el interés en esta tecnología sigue siendo fuerte.

2. DETALLES:

La red de generadores de deepnude opera bajo la misma marca "AI Nude" y se promueve a través de tácticas de SEO de sombrero negro para posicionar los sitios en lo más alto de los resultados de búsqueda.

Según Silent Push, FIN7 operaba directamente sitios como “aiNude[.]ai”, “easynude[.]website” y “nude-ai[.]pro”, que ofrecían pruebas o descargas gratuitas, pero en realidad solo difundían malware.

Los sitios web falsos permiten a los usuarios subir fotos con las que desean crear desnudos falsos. Sin embargo, una vez realizado el supuesto desnudo profundo, no se muestra en la pantalla. En su lugar, se le solicita al usuario que haga clic en un enlace para descargar la imagen generada.

Al hacerlo, el usuario será redirigido a otro sitio que muestra una contraseña y un enlace a un archivo protegido con contraseña alojado en Dropbox. Si bien este sitio sigue activo, el enlace de Dropbox ya no funciona.

Sin embargo, en lugar de una imagen de desnudo profundo, el archivo contiene el malware Lumma Stealer, que roba información. Cuando se ejecuta, el malware roba credenciales y cookies guardadas en navegadores web, billeteras de criptomonedas y otros datos del equipo.

Silent Push también vio algunos sitios que promocionaban un programa de generación de deepnude para Windows que en su lugar implementaría Redline Stealer y D3F@ck Loader, que también se utilizan para robar información de dispositivos comprometidos.

3. RECOMENDACIONES:

- Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña única para cada sitio, y permanecer alerta ante posibles intentos de phishing.
- Evitar abrir o descargar archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales. Verificar la fuente de información de tus correos entrantes.
- Utilizar una aplicación que le proporcione una capa adicional de protección escaneando e identificando aplicaciones potencialmente dañinas, detectando malware y advirtiendo actividades sospechosas.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/fin7-hackers-launch-deepfake-nude-generator-sites-to-spread-malware/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°228	Fecha: 02-10-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos de la serie 700 de SCHNEIDER Elektronik		
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:

Felix Eberstaller y David Schauer de Limes Security GmbH han reportado una vulnerabilidad de severidad **ALTA** de tipo autenticación faltante para función crítica que afecta a los dispositivos de la serie 700 de SCHNEIDER Elektronik. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante que tenga acceso a la red donde se encuentran los componentes de SCHNEIDER Elektronik causar una denegación de servicio mientras enumera el segmento de red.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-35293 de tipo autenticación faltante para función crítica, podría permitir a un atacante con acceso a la red donde se encuentran los componentes de SCHNEIDER Elektronik generar una condición de denegación de servicio (DoS) mientras enumera el segmento de red. Un atacante remoto no autenticado puede usar una vulnerabilidad de autenticación faltante para una función crítica para reiniciar o borrar los dispositivos afectados, lo que resulta en pérdida de datos y/o un ataque de DoS.

La serie 700 de SCHNEIDER Elektronik utiliza dos puertos para la comunicación entre controladores y para la comunicación con el software de programación. La comunicación con estos puertos puede producirse sin ningún tipo de autenticación. Esto lleva al hecho de que paquetes malformados o no intencionados pueden ser enviados y procesados por el controlador. Esto resulta en un comportamiento no intencionado del controlador que causa un reinicio y borra el sistema de archivos que contiene la lógica del programa.

A. Productos afectados:

- SCHNEIDER Elektronik serie 700, versiones anteriores a la 0.1.17.7.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.schneider-elektronik.de/wp-content/uploads/2024/07/SAR-202405-1.pdf

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°228	Fecha: 02-10-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos Sophos Intercept X para Windows		
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:

Sina Kheirkhah (@SinSinology) de watchTowr ha reportado una vulnerabilidad de severidad **ALTA** de tipo uso de componentes de terceros sin mantenimiento que afecta a los dispositivos de Sophos Intercept X para Windows con Central Device Encryption. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado escribir archivos arbitrarios en el sistema, lo que provocaría un gran impacto en la confidencialidad, la integridad y la disponibilidad.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-8885 de tipo uso de componentes de terceros sin mantenimiento que afecta al software Sophos Intercept X para Windows, podría permitir que un atacante con privilegios bajos aumente sus privilegios localmente en los sistemas Windows afectados. El atacante podría escribir archivos arbitrarios en el sistema, lo que provocaría un gran impacto en la confidencialidad, la integridad y la disponibilidad.

A. Productos afectados:

- Sophos Intercept X para Windows con Central Device Encryption 2024.2.0 y versiones anteriores.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. Asimismo, los clientes que utilizan la política de actualización predeterminada no necesitan realizar ninguna acción, ya que las actualizaciones de los paquetes recomendados se instalan automáticamente de forma predeterminada. Los clientes que utilicen paquetes de soporte a plazo fijo (FTS) o de soporte a largo plazo (LTS) deben actualizar su versión para recibir esta solución.

Fuente de Información:	• hxxps://www.sophos.com/en-us/security-advisories/sophos-sa-20241002-cde-lpe • hxxps://support.sophos.com/support/s/article/KBA-000002911?language=en_US

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°228	Fecha: 02-10-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades 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 múltiples vulnerabilidades de severidad **ALTA** de tipo desbordamiento de enteros, error de validación de entrada y control de seguridad implementado incorrectamente para el estándar en Google Chrome. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-7025 de tipo desbordamiento de enteros, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un desbordamiento de números enteros en el componente Layout de Google Chrome. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada, desencadenar un desbordamiento de números enteros y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-9369 de tipo error de validación de entrada, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta al procesar contenido HTML en Mojo. Chrome High. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada y ejecute código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2024-9370 de tipo control de seguridad implementado incorrectamente para el estándar, podría permitir a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a una implementación incorrecta en V8 en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y comprometer el sistema.

A. Productos afectados:

- Google Chrome: 100.0.4896.60 - 129.0.6668.72.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html • hxxp://crbug.com/368208152 • hxxp://crbug.com/367764861 • hxxp://crbug.com/368311899

Índice alfabético