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

203-2024-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°203	Fecha: 03-09-2024
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	'Jackpotting': La técnica con la que pueden sacar todo el dinero de un cajero sin que se den cuenta		
Tipo de Ataque	Malware	Abreviatura	Malware
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:

Los cibercriminales tienen en los cajeros automáticos un objetivo lucrativo y relativamente vulnerable, que han aprendido a explotar mediante una técnica conocida como jackpotting. Este método implica la utilización de malware para hacer que los cajeros automáticos expulsen todo o parte de su dinero, sin la necesidad de recurrir a tarjetas de crédito robadas o clonadas.

Aunque los primeros casos documentados datan de hace más de una década, los incidentes de jackpotting han aumentado en frecuencia y sofisticación en los últimos tiempos, afectando a entidades financieras en todo el mundo.

De hecho, el término "jackpotting" se popularizó en 2010, cuando el investigador de seguridad Barnaby Jack demostró durante la conferencia de ciberseguridad 'Black Hat' cómo un cajero automático podía ser manipulado para expulsar todo su efectivo.

También hay otros métodos como el 'Card skimming', o el 'shoulder surfing'.

2. DETALLES:

Consiste en utilizar un malware para que los cajeros automáticos expulsen una gran cantidad de dinero, sin necesidad de una tarjeta de crédito, ni tener que recurrir al robo con violencia o clonar las tarjetas de crédito.

El proceso de jackpotting generalmente involucra los siguientes pasos:

- **Acceso físico al cajero:** Los delincuentes suelen disfrazarse de técnicos para evitar levantar sospechas mientras abren un panel del cajero para acceder a los puertos USB internos.
- **Instalación del malware:** Una vez que tienen acceso físico, insertan un dispositivo USB que contiene el malware. Los ejemplos más notorios de este tipo de malware son Cutlet Maker y Ploutus. Estos programas maliciosos se instalan en el sistema del cajero, dándoles control sobre su funcionamiento.
- **Activación y control:** Con el malware instalado, los atacantes pueden usar comandos para hacer que el cajero expulse dinero. En algunos casos, esto se puede hacer de forma remota, pero normalmente requiere la presencia física de los delincuentes para monitorear y asegurar la operación.
- **Retiro del dinero:** Los cajeros infectados comienzan a dispensar billetes, que son recolectados por los atacantes o por 'mulas' de dinero, personas que recogen y transportan el efectivo sustraído.

Es un robo que no afecta tanto a los usuarios, si no a los bancos. Frente a ello, son las entidades bancarias las que tendrán que tomar medidas. Medidas como actualizar su software o incrementar la seguridad física, entre otras.

A continuación, se describen los malwares más destacados utilizados en estas operaciones criminales.

A. Ploutus

- Es uno de los malwares más avanzados utilizados en el jackpotting. Descubierto por primera vez en México en 2013, ha evolucionado a través de varias versiones:
- Ploutus-A: La primera versión, que requería la inserción de un CD en el cajero automático.
- Ploutus-B: Introducida en 2014, esta versión permitió la distribución a través de un teléfono móvil conectado por USB.
- Ploutus-D: La versión más reciente, lanzada en 2016, utiliza un ofuscador .NET para evitar la detección y es compatible con máquinas de 41 proveedores diferentes en 80 países.

B. Cutlet Maker

- Cutlet Maker es otro malware notable que ha ganado notoriedad en el mundo del jackpotting. Inicialmente vendido en foros clandestinos, este malware es conocido por su facilidad de uso y la poca necesidad de conocimientos técnicos avanzados para operarlo.
- Infección: Se introduce a través de una memoria USB conectada al cajero automático, junto con un teclado externo.
- Interfaz: Muestra un mensaje en la pantalla del cajero con una caricatura de un chef y un mensaje que dice “¡Ho-ho-ho! ¡Hagamos unas chuletas hoy!”.

C. WinPot

- WinPot, descubierto en 2018, está inspirado en Cutlet Maker pero con características adicionales que lo convierten en una herramienta muy poderosa para los cibercriminales.
- Funcionamiento: Convierte al cajero automático en una máquina tragamonedas, permitiendo la dispensación continua de billetes.
- Actualizaciones: Ha pasado por varias versiones, cada una mejorando la interfaz y los métodos de operación para evitar la detección y aumentar la efectividad.
- Método de infección: Al igual que otros malwares, requiere acceso físico al puerto USB del cajero.

D. EU ATM

- La cepa de malware EU ATM es una amenaza desvelada en estos últimos meses, dirigida específicamente a cajeros automáticos en Europa.

- Efectividad: Tiene una eficacia del 99% en cajeros europeos y del 60% en otras regiones.
- Capacidad de extracción: Permite retirar hasta 30.000 dólares (unos 28.000 euros) de un solo cajero.
- Basado en el estándar XFS: Este estándar proporciona una API para gestionar diferentes módulos internos de los cajeros, independientemente del fabricante.
- Automatización: La dispensación de dinero puede ser completamente automatizada, requiriendo solo la acción física de recoger los billetes.

Los principales cajeros vulnerables son conocidos con el nombre de Opteva, de los fabricantes Diebold Nixdorf Inc. y NCR Corp.

Aunque estos modelos ya no se fabrican, éstos aún pueden ser utilizados en distintas regiones del mundo.

En el caso de Ploutus, la variante de Ploutus D se diferencia en que utiliza componentes de Kalignite, un software muy utilizado en cajeros automáticos.

Ploutus D tiene un ejecutable y un launcher. El ejecutable puede ser lanzado como una aplicación independiente o como un servicio instalado desde el launcher.

El malware se ejecutará en segundo plano a la espera de una combinación de teclas que lo active, y así obtener el control de la máquina.

Cuando esto ocurre se despliega en la pantalla una interfaz personalizada que pide un código de autorización, si se da dicha autorización, el cajero muestra información como la cantidad de dinero que contiene.

Además, usara los componentes XFS de Kalignite para obtener acceso al dispensador del cajero.

De esta manera podrá lanzar distintos comandos que le permitan dispensar el dinero solicitado y así vaciar el cajero.

Finalmente, el malware da la opción de lanzar un mecanismo de limpieza que permita borrar todo rastro del ataque.

3. RECOMENDACIONES:

- Mantener el software de los cajeros actualizado y protegido con soluciones antimalware es crucial.
- Mejorar la seguridad física de los cajeros mediante la instalación de cámaras de vigilancia, el refuerzo de los gabinetes y la contratación de personal de seguridad para monitorear los cajeros.
- Implementar mecanismos que dificulten el acceso físico no autorizado a los componentes internos del cajero, como el uso de cerraduras mejoradas y alarmas de seguridad.
- Asegurar que los datos del cajero estén cifrados para proteger la información sensible y evitar que los atacantes puedan acceder a los sistemas de control.
- Evitar la presencia muy cercana de personas desconocidas y evitar recibir ayuda de desconocidos.
- Cambiar con frecuencia las claves de las tarjetas.
- No ingresar la tarjeta si es que se encuentra otro objeto en la ranura de ingreso.
- No brindar la tarjeta a nadie y nunca perderla de vista.
- Asegurarse de cerrar sesión al terminar de usar el cajero.
- Evitar que otras personas vean los botones que presiona al ingresar su DNI o clave secreta.

Fuente de Información:	• hxxps://www.genbeta.com/a-fondo/que-jackpotting-tecnica-robo-que-permite-vaciar-cajeros-mediante-malware • hxxps://www.noticiasdenavarra.com/ciencia-y-tecnologia/2024/09/02/jackpotting-tecnica-sacar-dinero-cajero-sin-darse-cuenta-8643247.html • Análisis propio de redes sociales y Ciberpatrullaje

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°203	Fecha: 03-09-2024 Página: 7 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en el editor de gadgets OpenSocial de varios productos de Cisco		
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 ha reportado dos vulnerabilidades de severidad **MEDIA** de tipo autenticación faltante para función crítica y neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) en la interfaz de administración basada en web de Cisco Finesse, Cisco Virtualized Voice Browser y Cisco Unified Customer Voice Portal (CVP). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar un ataque de secuencias de comandos entre sitios (XSS) y obtener información confidencial al aprovechar una falla en el mecanismo de autenticación.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2021-1245 de tipo secuencias de comandos entre sitios en la interfaz de administración basada en web de Cisco Finesse y Cisco Unified CVP OpenSocial Gadget Editor, podría permitir que un atacante remoto no autenticado realice un ataque de secuencias de comandos entre sitios (XSS) contra un usuario de la interfaz. La vulnerabilidad existe porque la interfaz de administración basada en la web no valida correctamente la información proporcionada por el usuario. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que haga clic en un vínculo creado. Si lo hiciera, podría permitirle ejecutar código de script arbitrario en el contexto de la interfaz o acceder a información confidencial basada en el navegador.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2021-1246 de acceso no autenticado en la interfaz de administración web de Cisco Finesse, Cisco Virtualized Voice Browser y Cisco Unified CVP OpenSocial Gadget Editor, podría permitir que un atacante remoto no autenticado acceda al Editor de Gadgets de OpenSocial sin proporcionar credenciales de usuario válidas. La vulnerabilidad se debe a la falta de autenticación para una sección específica de la interfaz de administración basada en web. Un atacante podría aprovechar esta vulnerabilidad accediendo a una URL creada. Si lo hiciera, podría obtener acceso a una sección de la interfaz, que podría utilizar para obtener información potencialmente confidencial y crear archivos XML arbitrarios.

Cisco indico que las vulnerabilidades dependen unas de otras; es necesario explotar una de ellas para explotar la otra.

A. Productos afectados:

- Cisco Finesse, anteriores a la versión 12.0(1) ES3 y la versión 12.5(1).
- Cisco Virtualized Voice Browser, anteriores a la versión 12.6(1).
- Cisco Unified CVP, versión 12.6(2) ES4 a 12.6(2) ES17.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multi-vuln-finesse-qp6gbUO2

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°203	Fecha: 03-09-2024
		Página: 8 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Serie LINX de LOYTEC electronics GmbH		
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:

El investigador Chizuru Toyama de TXOne Networks, ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo transmisión de información confidencial en texto claro, falta de autenticación para funciones críticas, almacenamiento de información confidencial en texto claro y control de acceso inadecuado en diversos productos de LOYTEC. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto revelar información confidencial, realizar modificaciones en un dispositivo afectado u obtener control total de la configuración del dispositivo LOYTEC.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46380 de tipo transmisión de información sensible en texto claro, existe debido a que los dispositivos LOYTEC LINX-212 firmware 6.2.4, LVIS-3ME12-A1 firmware 6.2.2 y LIOB-586 firmware 6.2.3 envían solicitudes de cambio de contraseña a través de HTTP de texto sin formato.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46381 de tipo falta autenticación para función crítica, existe debido a que los dispositivos LOYTEC LINX-212 firmware 6.2.4, LVIS-3ME12-A1 firmware 6.2.2 y LIOB-586 firmware 6.2.3 carecen de autenticación para la versión preinstalada de LWEB-802 a través de una URI lweb802_pre/. Un atacante no autenticado puede editar cualquier proyecto (o crear un nuevo proyecto) y controlar su GUI.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46382 de tipo transmisión de información sensible en texto claro, existe debido a que los dispositivos LOYTEC LINX-212 firmware 6.2.4, LVIS-3ME12-A1 firmware 6.2.2 y LIOB-586 firmware 6.2.3 utilizan HTTP de texto sin formato para iniciar sesión.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46383 de tipo transmisión de información sensible en texto claro, existe debido a que el configurador LINX 7.4.10 de LOYTEC electronics GmbH utiliza autenticación básica HTTP, que transmite nombres de usuario y contraseñas en texto claro codificado en base64 y permite a atacantes remotos robar la contraseña y obtener control total de la configuración del dispositivo LOYTEC.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46384 de tipo almacenamiento de información sensible en texto claro, existe debido a que el configurador LINX 7.4.10 de LOYTEC electronics GmbH es vulnerable a permisos inseguros. El almacenamiento de credenciales en texto sin formato permite a atacantes remotos revelar la contraseña de administrador y eludir una autenticación para iniciar sesión.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46385 de tipo transmisión de información sensible en texto claro, existe debido a que el configurador LINX 7.4.10 de LOYTEC electronics GmbH es vulnerable a permisos inseguros. Se pasa una credencial de administrador como valor de parámetros de URL sin cifrado, por lo que permite a atacantes remotos robar la contraseña y obtener control total de la configuración del dispositivo LOYTEC.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46386 de tipo almacenamiento de información sensible en texto claro, existe debido a que el firmware 6.2.4 de LINX-212 y el firmware 7.2.4 de LINX-151 de LOYTEC electronics GmbH son vulnerables a permisos inseguros a través del archivo registration.xml. Esta vulnerabilidad permite a atacantes remotos revelar credenciales de cuentas de clientes SMTP y eludir la autenticación de correo electrónico.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46387 de tipo control de acceso inadecuado, existe debido a que el firmware 6.2.4 de LINX-212 y el firmware 7.2.4 de LINX-151 de LOYTEC electronics GmbH son vulnerables a un control de acceso incorrecto a través del archivo dpal_config.zml. Esta vulnerabilidad permite a atacantes remotos divulgar información confidencial sobre la configuración de los puntos de datos del dispositivo LOYTEC.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46388 de tipo almacenamiento de información sensible en texto claro, existe debido a que LOYTEC electronics GmbH LINX-212 6.2.4 y LINX-151 7.2.4 son vulnerables a permisos inseguros a través del archivo dpal_config.zml. Esta vulnerabilidad permite a atacantes remotos revelar credenciales de cuentas de clientes SMTP y eludir la autenticación de correo electrónico.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-46389 de tipo control de acceso inadecuado, existe debido a que el firmware 6.2.4 de LINX-212 y el firmware 7.2.4 de LINX-151 de LOYTEC electronics GmbH son vulnerables a un control de acceso incorrecto a través del archivo Registry.xml. Esta vulnerabilidad permite a atacantes remotos divulgar información confidencial sobre la configuración de LINX.

A. Productos afectados:

- LINX-151: Todas las versiones.
- LINX-212: Todas las versiones.
- LVIS-3ME12-A1: Todas las versiones.
- LIOB-586: Todas las versiones.
- LIOB-580 V2: Todas las versiones.
- LIOB-588: Todas las versiones.
- Configurador L-INX: Todas las versiones.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la versión de firmware 8.2.8 que aborda esta vulnerabilidad.
- Deshabilitar HTTP en el dispositivo LOYTEC, para CVE-2023-46380, CVE-2023-46382, CVE-2023-46383, CVE-2023-46385, según lo recomendado por la guía de fortalecimiento de seguridad de LOYTEC.
- Actualizar al firmware más reciente, para CVE-2023-4638. Se han reforzado los permisos en proyectos LWEB.
- Actualizar al firmware más reciente, para CVE-2023-46387, CVE-2023-46389. El firmware actual protege el archivo registration.xml y dpal_config.zml mediante acceso de administrador.
- Actualizar el parche que el proveedor publicará en LINX Configurator, para CVE-2023-46384.
- Actualizar el parche que el proveedor publicará en LINX, para las vulnerabilidades CVE-2023-46386, CVE-2023-46388. El firmware de LINX implementará el almacenamiento cifrado de credenciales SMTP. El parche se publicará como actualización del firmware de LINX.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-247-01 • hxxps://www.loytec.com/dl/manual/LINX_LGATE_User_Manual.pdf

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°203	Fecha: 03-09-2024 Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en múltiples versiones de VMware Fusion		
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 reportado una vulnerabilidad de severidad **ALTA** de tipo validación de entrada incorrecta que afecta a VMware Fusion. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local la ejecución de código arbitrario, lo que podría comprometer la confidencialidad, la integridad y la disponibilidad del sistema.

2. DETALLES:

VMware Fusion es un software de virtualización para macOS. Permite a los usuarios ejecutar múltiples sistemas operativos en su propio equipo. Incluidos Windows y Linux, y todo corriendo en un solo dispositivo Apple. VMware Fusion crea una máquina virtual en el equipo del usuario.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-38811 de tipo validación de entrada incorrecta, podría permitir a un atacante remoto la ejecución de código debido al uso de una variable de entorno insegura. Un actor malintencionado con privilegios de usuario estándar puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de la aplicación Fusion. Esto podría provocar un acceso no autorizado a datos confidenciales o recursos del sistema, lo que podría comprometer todo el sistema.

Aunque la vulnerabilidad en sí no permite la explotación remota, puede servir como punto de apoyo para los atacantes. Una vez dentro del sistema, pueden aprovechar otras vulnerabilidades para escalar privilegios y obtener un acceso más profundo al sistema o la red.

Asimismo, los atacantes podrían modificar las configuraciones del sistema o instalar software malicioso, lo que provocaría una mayor explotación o interrupción de los servicios. Esto podría afectar la confiabilidad e integridad de las máquinas virtuales administradas por VMware Fusion.

Cabe indicar que las actualizaciones y las prácticas de seguridad periódicas son esenciales para mantener la seguridad de los sistemas frente a las amenazas en constante evolución.

A. Productos afectados:

- VMware Fusion 13.x versiones anteriores a 13.6 en MacOS.

3. RECOMENDACIONES:

- Actualizar a la versión 13.6 o a una posterior que VMware ha publicado para mitigar el riesgo.
- Restringir el acceso de los usuarios y supervisar las actividades sospechosas, en caso no se pueda realizar una actualización inmediata.
- Revisar y auditar periódicamente el uso de las variables de entorno dentro de la aplicación.

Fuente de Información:	• hxxps://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24939

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°203	Fecha: 03-09-2024 Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Google ChromeOS		
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 reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo confusión de tipos y control de seguridad implementado incorrectamente para el estándar en el motor V8 de Google Chrome. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-7971 de tipo confusión de tipos, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de confusión de tipos dentro del motor V8. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, generar un error de confusión de tipos y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-7965 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.

Estas vulnerabilidades vienen siendo explotados activamente en la naturaleza.

A. Productos afectados:

- Sistema operativo Chrome: anterior a 120.0.6099.331.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda en la 1era esta vulnerabilidad.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2024/09/long-term-support-channel-update-for.html

Índice alfabético