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

107-2024-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°107	Fecha: 08-05-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los Piratas Informáticos abusan de los Anuncios de búsqueda de Google para distribuir Malware empaquetado en MSI		
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:

Se ha descubierto que los piratas informáticos explotan los anuncios de búsqueda de Google para distribuir malware a través de paquetes MSI (Microsoft Installer).

Esta campaña, que involucra el cargador de malware conocido como FakeBat, apunta a usuarios desprevenidos haciéndose pasar por descargas de software legítimas.

2. DETALLES:

El ataque comienza con un anuncio de búsqueda de Google que parece legítimo y utiliza la dirección real del sitio web de un software popular como Notion.

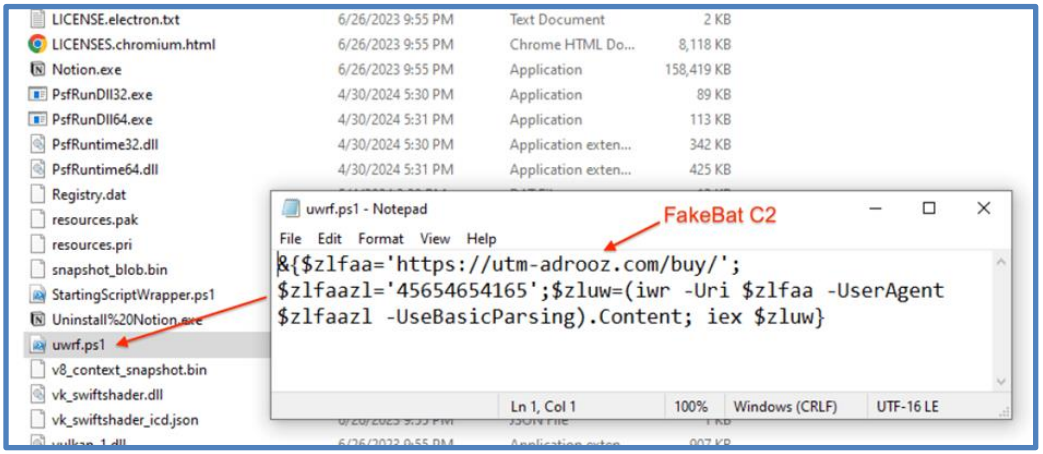
Al hacer clic en el anuncio, se accede a un sitio de phishing alojado en una URL engañosa que se parece al sitio genuino.

El sitio solicita a los usuarios que descarguen lo que parece ser un instalador de software estándar en formato MSIX, firmado con el nombre aparentemente creíble "Forth View Designs Ltd".

Al ejecutar el instalador de MSIX, se activa un script de PowerShell malicioso oculto.

Este script se encarga de conectarse al servidor de comando y control (C2) de FakeBat, iniciando la descarga de una carga útil secundaria conocida como zgRAT.

Los comandos de PowerShell ejecutados durante este proceso están diseñados para eludir las medidas de seguridad locales e inyectar el malware zgRAT directamente en los procesos del sistema, tomando efectivamente el control de la máquina infectada.



La campaña utiliza un servicio de seguimiento de clics para gestionar la eficacia del anuncio y filtrar el tráfico no deseado. Este paso implica un dominio intermediario que separa la URL maliciosa del anuncio de Google, mejorando el sigilo del ataque.

Una vez instalado el malware, el script de PowerShell llega al servidor FakeBat C2, que dicta las acciones posteriores, incluida la entrega de la carga útil zgRAT.

ThreatDown, una empresa de ciberseguridad, bloqueó el C2 utilizado en esta campaña y registró la progresión del ataque desde la ejecución inicial de MSIX hasta el despliegue final de la carga útil.

Indicadores de Compromiso:

Sitio web de noción falsa:

- notilion[.]co

Instalador de FakeBat:

- hxxps[://]sivaspastane[.]com/Notion-x86[.]msix

FakeBat SHA256:

- 80f4405270b8fd7f557c6831dd2785b55fdee43d48d967401a8b972e147be948

Ruta de ejecución de MSIX:

- C:\ARCHIVOS DE PROGRAMA\WINDOWSAPPS\NOTIONLAB.NOTION_2.0.47.1_X86__MRGZP1VAGPXMP\AI_STUBS\AISTUBX86.EXE

FakeBat C2:

- utm-adrooz[.]com

Host de descarga zgRAT:

- startupzonechanpatia[.]com

zgRAT SHA256:

- 5102b64a838bd84f4273bce2a0bda67df77fdb1a33a2b939988ccb51f2246e07

zgRAT C2:

- shatterbreathepsw[.]shop
- productivelookewr[.]shop
- tolerailusidjukl[.]shop
- shortsvelventysjo[.]shop
- increíbleextedwj[.]shop
- alcojoldwograpciw[.]shop
- liabilitynighstjsko[.]shop
- demonstationfukewko[.]shop

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados.
- Implementar sistemas de detección y respuesta de puntos finales (EDR) para monitorear y bloquear este tipo de actividades maliciosas.
- Restringir o controlar el uso de archivos MSIX a través de políticas de grupo y distribuir instaladores de software a través de un repositorio interno de la empresa para evitar los riesgos asociados con anuncios maliciosos.
- Diseñar una estrategia de concientización y capacitación que incluya la responsabilidad en el manejo de la información.

Fuente de Información:	• hxxps://gbhackers.com/abuse-google-search-ads/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2024 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades críticas en navegadores que utilizan PDF.Js y React-PDF		
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 descubierto una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución de código arbitrario que afecta a múltiples navegadores y aplicaciones que utilizan React-PDF. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario al abrir un archivo PDF malicioso. Cabe indicar que PDF.js permite a los navegadores representar archivos PDF sin complementos ni software externo.

2. DETALLES:

Se ha descubierto una nueva vulnerabilidad crítica en PDF.js, que podría permitir que un actor de amenazas ejecute código arbitrario al abrir un PDF malicioso. PDF.js permite a los navegadores representar archivos PDF sin complementos ni software externo. Esta vulnerabilidad afecta a múltiples navegadores y aplicaciones que utilizan React-PDF.

Cabe indicar que Mozilla PDF.js es la biblioteca original de código abierto que se centra en representar documentos PDF dentro de un navegador, y React-PDF PDF.js se basa en Mozilla PDF.js y se utiliza para integrar PDF.js en aplicaciones React. Esta vulnerabilidad podría afectar a millones de usuarios de PDF, así como a las aplicaciones React que utilizan React PDF.

PDF.js es utilizado por muchos navegadores como Mozilla Firefox, Safari, Google Chrome y Edge, lo que hace que su panorama de amenazas sea más grande. Sin embargo, esta vulnerabilidad ha sido reparada por Wojciech Maj, el mantenedor del proyecto React-pdf.

PDF.js está integrado en Mozilla Firefox como visor de PDF predeterminado. Había dos vulnerabilidades asociadas con esta vulnerabilidad: CVE-2024-34342 y CVE-2024-4367.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-34342, está relacionada con reaccionar-pdf que puede ser explotada por un actor de amenazas utilizando un archivo PDF malicioso. Sin embargo, existen ciertos requisitos previos para explotarlo por completo, incluido el uso de PDF.js para cargar el PDF malicioso y la configuración de PDF.js con isEvalSupported establecido en "true". Si existen estas dos condiciones, entonces el actor de la amenaza podrá ejecutar JavaScript en el contexto del dominio de alojamiento.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4367, existe en la biblioteca PDF.js de Mozilla y podría permitir que un actor de amenazas ejecute código arbitrario en el contexto del usuario que ha iniciado sesión. Además, según el privilegio del usuario, es posible que un actor de amenazas aproveche esta vulnerabilidad e "instale programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los derechos de usuario". La vulnerabilidad existe por la misma razón que reaccionar-pdf PDF.js que tiene isEvalSupported establecido en verdadero como valor predeterminado.

A. Productos afectados:

- Esta vulnerabilidad afecta a múltiples navegadores como Mozilla Firefox, Safari, Google Chrome, Edge y aplicaciones que utilizan React-PDF.

3. RECOMENDACIÓN:

- Actualizar los productos a las últimas versiones para evitar la explotación de estas vulnerabilidades por parte de actores de amenazas.

Fuente de Información:	• hxxps://gbhackers.com/pdf-js-react-pdf-vulnerabilities-threat/ • hxxps://github.com/mozilla/pdf.js • hxxps://nvd.nist.gov/vuln/detail/CVE-2024-34342 • hxxps://www.cisecurity.org/advisory/a-vulnerability-in-mozilla-pdfjs-could-allow-for-arbitrary-code-execution_2024-046

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2024 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas en el software de gestión de UPS CyberPower		
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 múltiples vulnerabilidades de severidad **CRÍTICA** de tipo uso de contraseña codificada, uso de credenciales codificadas, código de depuración activo, recorrido de ruta relativa, inyección SQL, uso de clave criptográfica codificada, autorización inadecuada y almacenamiento de contraseñas en formato recuperable en el software de gestión UPS CyberPower. La explotación de las vulnerabilidades en PowerPanel vulnerable podría permitir a un atacante eludir potencialmente la autenticación y obtener privilegios de administrador, que podrían utilizarse para escribir archivos arbitrarios en el servidor para la ejecución de código, obtener acceso a información confidencial, hacerse pasar por cualquier cliente para enviar datos maliciosos y obtener acceso al servidor de prueba o de producción.

2. DETALLES:

El software de gestión de UPS es empleado por un amplio espectro de usuarios, que abarca centros de datos, sectores de fabricación críticos, instalaciones de atención médica, instituciones educativas, agencias gubernamentales y más, para mantener operaciones de misión crítica ininterrumpidas.

El software de administración de UPS, como PowerPanel, está diseñado para brindar administración de energía avanzada para sistemas de suministro de energía ininterrumpida, unidades de distribución de energía o interruptores de transferencia automática.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-34025 de tipo uso de contraseña codificada, se debe a que el código de la aplicación contiene un conjunto codificado de credenciales de autenticación. Esto podría provocar que un atacante eluda la autenticación y obtenga privilegios de administrador.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-32053 de tipo uso de credenciales codificadas se debe a que la plataforma utiliza credenciales codificadas para autenticarse en la base de datos, otros servicios y la nube. Esto podría dar lugar a que un atacante obtenga acceso a servicios con los privilegios de una aplicación empresarial Powerpanel.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-32047 de tipo código de depuración activo, se debe a que las credenciales codificadas para el servidor de prueba se pueden encontrar en el código de producción. Esto podría provocar que un atacante obtenga acceso al servidor de prueba o de producción.

Para las demás vulnerabilidades se le asigno los siguientes identificadores: CVE-2024-33615, CVE-2024-31856, CVE-2024-31410, CVE-2024-31409 y CVE-2024-32042.

Estas vulnerabilidades representan un riesgo grave para la integridad y confiabilidad de los sistemas de infraestructura crítica (CI), exponiéndolos potencialmente a la explotación por parte de actores maliciosos.

Por otro lado, los investigadores de CRIL han estado monitoreando de cerca las afirmaciones de los hacktivistas de atacar dispositivos del Sistema de Control Industrial (ICS) expuestos a Internet. En campañas anteriores lanzadas por grupos hacktivistas como GhostSec, SigedSec, TeamOneFist, etc., los ciberataques a sistemas UPS se han convertido en un vector clave en tales campañas para causar interrupciones masivas y ganar notoriedad a partir de dichos ataques. Aunque el impacto de tales afirmaciones sigue siendo cuestionable, la exposición y el acceso directo de los sistemas UPS a un atacante es un escenario profundamente preocupante.

La campaña OpColombia lanzada por SiegdSec en colaboración con GhostSec y múltiples campañas lanzadas por TeamOneFist en respuesta a la guerra Rusia-Ucrania en 2023 son algunos incidentes notables en los que supuestamente se atacaron sistemas UPS fabricados por Schneider Electric, Powest y APC.

A. Productos afectados:

- PowerPanel business: 4.9.0 y anteriores.

3. RECOMENDACIONES:

- Implementar una sólida estrategia de gestión de parches para abordar rápidamente las vulnerabilidades en el software y los sistemas. Asegurarse de que los parches de seguridad se apliquen periódicamente a todos los dispositivos y aplicaciones, priorizando las actualizaciones críticas para mitigar los riesgos potenciales de manera efectiva.
- Realizar auditorías de seguridad periódicas y ejercicios de pruebas de penetración para evaluar la efectividad de los controles de seguridad existentes e identificar vulnerabilidades. Revisar periódicamente las configuraciones, políticas y procedimientos para garantizar el cumplimiento de las mejores prácticas de seguridad y los requisitos reglamentarios.
- Utilizar herramientas de gestión de activos y técnicas de descubrimiento de redes para mantener un inventario preciso de todos los dispositivos y aplicaciones dentro del entorno. Mejorar la visibilidad de las configuraciones, vulnerabilidades y dependencias de los activos para facilitar una gestión de riesgos y una respuesta a incidentes eficaces.
- Implementar la autenticación multifactor (MFA) para todo el acceso remoto a la red de tecnología operativa (OT), incluidas las conexiones desde la red de TI y las redes externas, para mejorar la seguridad.

Fuente de Información:	• hxxps://cyble.com/blog/uninterrupted-power-supply-ups-a-silent-threat-to-critical-infrastructure-resilience/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°107	Fecha: 08-05-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Apple iTunes		
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 restricción inadecuada de operaciones dentro de los límites de un búfer de memoria en Apple iTunes. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-27793 de tipo desbordamiento de búfer, existe debido a un error de límite al procesar archivos. Un atacante remoto puede crear un archivo multimedia especialmente diseñado, engañar a la víctima para que lo abra, provocar daños en la memoria y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total del sistema vulnerable.

El error de sebe a que el producto realiza operaciones en un búfer de memoria, pero puede leer o escribir en una ubicación de memoria que esté fuera del límite previsto del búfer.

A. Productos afectados:

- iTunes: 12.0 - 12.13.1.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://support.apple.com/en-us/HT214099

Índice alfabético