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

195-2024-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°195	Fecha: 23-08-2024 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Descarga de películas piratas viene con malware		
Tipo de Ataque	Stealers	Abreviatura	Stealers
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

Investigadores de ciberseguridad han descubierto cómo se utilizan películas piratas como anzuelo para descargar un malware del tipo info stealers.

2. **DETALLES:**

"Este dropper se descrifra en memoria y ejecuta un download basado en PowerShell", dijo Mandiant, propiedad de Google. "Este descargador basado en PowerShell está siendo rastreado como PEAKLIGHT".

Algunas de las cepas de malware distribuidas mediante esta técnica son Lumma Stealer, Hijack Loader y CryptBot, todos los cuales se anuncian bajo el modelo de malware como servicio (SaaS).

El punto de partida de la cadena de ataque es un archivo de acceso directo de Windows (LNK) que se descarga mediante técnicas de descarga no autorizada, por ejemplo, cuando los usuarios buscan una película en los motores de búsqueda. Vale la pena señalar que los archivos LNK se distribuyen en archivos ZIP disfrazados de películas pirateadas.

El archivo LNK se conecta a una red de entrega de contenido (CDN) que aloja un dropper de JavaScript de solo memoria ofuscado. Posteriormente, el dropper ejecuta el script de descarga PEAKLIGHT PowerShell en el host, que luego se comunica con un servidor de comando y control (C2) para recuperar cargas útiles adicionales.

Mandiant dijo que identificó diferentes variaciones de los archivos LNK, algunos de los cuales aprovechan los asteriscos (*) como comodines para iniciar el binario mshta.exe legítimo para ejecutar discretamente código malicioso recuperado de un servidor remoto.

De manera similar, se ha descubierto que los droppers incorporan cargas útiles de PowerShell con codificación hexadecimal y base64 que finalmente se descomprimen para ejecutar PEAKLIGHT, que está diseñado para entregar malware de siguiente etapa en un sistema comprometido mientras se descarga simultáneamente un avance de película legítimo, probablemente como una artimaña.

"PEAKLIGHT es un download ofuscado basado en PowerShell que forma parte de una cadena de ejecución de múltiples etapas que verifica la presencia de archivos ZIP en rutas de archivos codificadas", dijeron los investigadores de Mandiant, Aaron Lee y Praveeth D'Souza. "Si los archivos no existen, el programa de descarga se comunicará con un sitio CDN y descargará el archivo alojado remotamente y lo guardará en el disco".

3. **RECOMENDACIONES:**

- Descargar archivos o aplicaciones únicamente de sitios web confiables y de buena reputación. Evitar hacer clic en enlaces o anuncios sospechosos, que provengan de correos electrónicos, mensajes de texto o mensajes de redes sociales que soliciten información personal.
- Verificar la autenticidad de los sitios web.
- Utilizar contraseñas seguras y autenticación de dos factores (2FA) para las cuentas financieras.
- Mantener el software actualizado. Actualizar periódicamente el sistema operativo, navegador y software antivirus para protegerse contra las últimas amenazas.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2024/08/toma-descarga-peliculas-piratas-e.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°195	Fecha: 23-08-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el módulo 5015 – AENFTXT de Rockwell Automation		
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 en el módulo 5015 – AENFTXT de Rockwell Automation, una parte de los módulos de E/S FLEXHA 5000. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-6089 de tipo validación de entrada incorrecta en el módulo 5015 – AENFTXT de Rockwell Automation, podría permitir a un atacante remoto generar una condición de DoS.

Existe una vulnerabilidad de validación de entrada en los productos afectados cuando se envía un paquete PTP manipulado, lo que provoca que el adaptador secundario presente una falla grave no recuperable. Si se explota, se requiere apagar y encender el producto para recuperarlo.

A. Productos afectados:

- Rockwell Automation 5015 - AENFTXT, versión 2.011.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión de firmware v2.012 que aborda esta vulnerabilidad.
- Implementar las mejores prácticas de seguridad sugeridas para minimizar el riesgo de vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-235-02 • hxxps://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°195	Fecha: 23-08-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el complemento LiteSpeed Cache de LiteSpeed Technologies para WordPress		
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 asignación incorrecta de privilegios en el complemento LiteSpeed Cache de LiteSpeed Technologies para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto elevar los privilegios en el sistema afectado.

2. **DETALLES:**

LiteSpeed Cache, desarrollado por LiteSpeed Technologies, es una potente solución de almacenamiento en caché diseñada para optimizar el rendimiento de los sitios web, en particular los creados con WordPress. Está disponible como un complemento gratuito y de código abierto que mejora significativamente la velocidad de carga de las páginas mediante el uso de almacenamiento en caché a nivel de servidor.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-28000 de tipo asignación incorrecta de privilegios en el complemento LiteSpeed Cache, podría permitir a un atacante remoto aumentar los privilegios en el sistema.

La vulnerabilidad existe debido a un hash de seguridad débil en una función de simulación de usuario. Un atacante remoto puede obtener privilegios elevados en el sistema de destino.

A. **Productos afectados:**

- Caché LiteSpeed: 1.0.15 - 6.3.0.1.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• http://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-6-3-0-1-unauthenticated-privilege-escalation-vulnerability?_s_id=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°195	Fecha: 23-08-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en el servicio LDB de Qualcomm Wi-Fi SON		
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 **CRÍTICA** de tipo validación de entrada incorrecta en el servicio LDB de Qualcomm Wi-Fi SON. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante adyacente a la red ejecutar código arbitrario en instalaciones afectadas de múltiples conjuntos de chips Qualcomm.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-21473 de tipo validación de entrada incorrecta del servicio LDB de Qualcomm Wi-Fi SON, podría permitir a un atacante adyacente a la red ejecutar código arbitrario en instalaciones afectadas de múltiples conjuntos de chips Qualcomm. No se requiere autenticación para explotar esta vulnerabilidad.

La falla específica existe dentro del servicio Qualcomm LDB. El problema es el resultado de la falta de una validación adecuada de los datos proporcionados por el usuario antes de su posterior procesamiento. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de la raíz.

A. Productos afectados:

- Múltiples versiones Chipsets de Wi-Fi SON.

3. RECOMENDACIÓN:

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

Fuente de Información:	• https://docs.qualcomm.com/product/publicresources/securitybulletin/april-2024-bulletin.html

Índice alfabético