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

194-2024-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°194	Fecha: 22-08-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Malware vulnera contraseñas débiles de PostgreSQL para minería de criptomonedas		
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:**

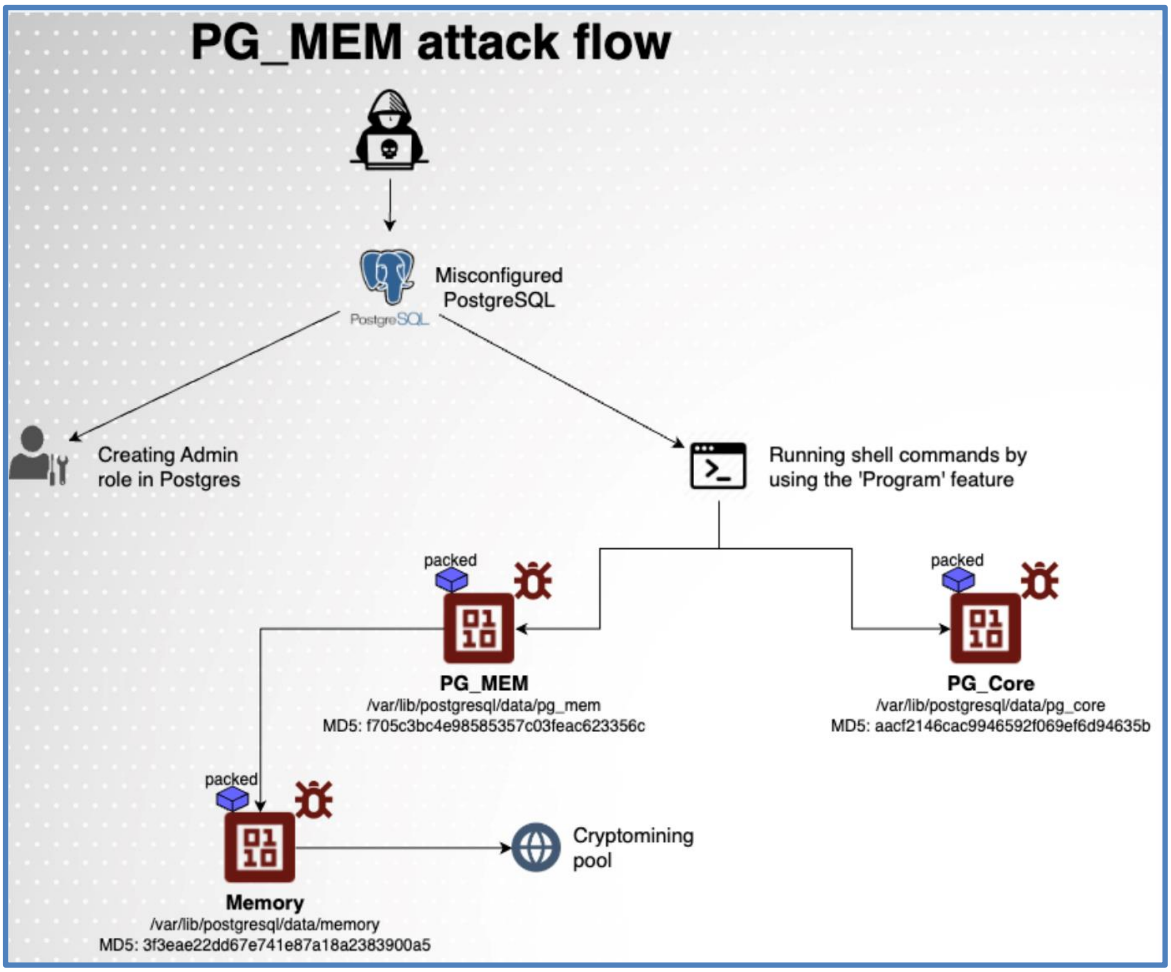
PostgreSQL es un sólido sistema de gestión de bases de datos relacionales de código abierto conocido por su flexibilidad y confiabilidad.

Los investigadores de ciberseguridad de Aqua Nautilus han descubierto un nuevo malware que apunta a bases de datos para instalar software de minería de criptomonedas. Denominado PG_MEM, el malware podría afectar potencialmente a cualquiera de las más de 800,000 bases de datos gestionadas por PostgreSQL si tienen contraseñas débiles.

2. **DETALLES:**

El uso de malware para minar criptomonedas se conoce como cryptojacking. El malware de cryptojacking también puede instalarse en computadoras personales. Está ocurriendo con mayor frecuencia.

El flujo de ataque de PG_MEM



Etapa 1: Ataque de fuerza bruta

La etapa inicial del ataque PG_MEM implica un intento de fuerza bruta para obtener acceso a la base de datos PostgreSQL.

Esto implica numerosos intentos de inicio de sesión hasta que el atacante adivine con éxito el nombre de usuario y la contraseña.

Una vez obtenido el acceso, el atacante puede ejecutar comandos y manipular el entorno de la base de datos.

Etapa 2: Ganando Persistencia

Después de obtener acceso, el atacante crea un rol de superusuario en la base de datos, lo que le permite mantener el control y evadir la detección.

Esto implica ejecutar comandos SQL para manipular los roles y privilegios de los usuarios, lo que garantiza que el atacante conserve el acceso y restringe el acceso a otros.

Etapa 3: Descubrimiento del sistema y entrega de la carga útil

El atacante recopila información del sistema y distribuye cargas maliciosas explotando las características de PostgreSQL.

Se descargaron dos archivos, incluido el malware PG_Core, del servidor remoto del atacante y se ejecutaron para minar criptomonedas.

El malware está inteligentemente disfrazado y se ejecuta utilizando comandos codificados para evitar ser detectado.

PG_MEM actúa como un cuentagotas para un minero de criptomonedas conocido como XMRIG. Una vez implementado, optimiza la operación de minería aprovechando los recursos del sistema.

El ataque PG_MEM se alinea con varias técnicas descritas en el marco MITRE ATT&CK.

Entre ellas se incluyen la explotación de aplicaciones públicas, la ejecución de intérpretes de comandos y secuencias de comandos, la manipulación de cuentas y el secuestro de recursos. Comprender estas técnicas puede ayudar a desarrollar estrategias de defensa eficaces.

3. RECOMENDACIONES:

- Adoptar un enfoque de defensa en profundidad para protegerse contra PG_MEM y amenazas similares.
- Implementar políticas de contraseñas seguras.
- Ejecutar auditorías de seguridad periódicas.
- Usar herramientas que puedan detectar comportamientos sospechosos en tiempo real.

Fuente de Información:	• hxxps://gbhackers.com/pg_mem-a-malware-postgres/ • hxxps://es.cointelegraph.com/news/pg-mem-malware-targets-postgresql-databases-crypto-mining

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°194	Fecha: 22-08-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en múltiples versiones PHP		
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 equipo Threat Hunter de Symantec ha detectado una vulnerabilidad de severidad **CRÍTICA** de tipo Inyección de comando del sistema operativo en múltiples versiones de PHP al utilizar Apache y PHP-CGI en Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código en servidores PHP que utilizan sistemas operativos Windows.

2. DETALLES:

El equipo Threat Hunter de Symantec ha descubierto que actores de amenazas no identificados han desplegado un sofisticado malware de tipo backdoor (puerta trasera), denominado "Msupedge", en equipos con sistemas Windows. Los atacantes han explotado la vulnerabilidad de ejecución remota de código PHP CVE-2024-4577.

El malware fue desplegado como dos bibliotecas de vínculos dinámicos (weblog.dll y wmiclnt.dll), siendo la primera cargada por el proceso Apache httpd.exe, lo que le permite integrarse en los sistemas comprometidos de manera furtiva.

Los expertos indicaron, lo que distingue a "Msupedge" de otros malware es su uso del tráfico DNS para comunicarse con su servidor de comando y control (C&C). Aunque esta técnica ha sido utilizada por otros actores de amenazas, su aparición en la red sigue siendo relativamente anómala. "Msupedge" implementa la tunelización DNS utilizando la herramienta de código abierto dnscat2, lo que permite encapsular datos dentro de consultas y respuestas DNS, proporcionando así un canal encubierto para recibir comandos del servidor de C&C.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4577 de tipo inyección de comandos PHP-CGI en el sistema operativo, podría permitir la ejecución remota de código en servidores PHP que utilizan sistemas operativos Windows. Esta falla afecta varias versiones de PHP y puede ser explotada fácilmente, por lo que se recomienda actualizar a las versiones más recientes para mitigar los riesgos.

Esta vulnerabilidad permite a los atacantes no autenticados ejecutar código arbitrario en servidores PHP a través de un ataque de inyección de argumentos. La vulnerabilidad afecta todas las versiones de PHP instaladas en sistemas operativos Windows.

A. Productos afectados:

- PHP 8.3 < 8.3.8.
- PHP 8.2 < 8.2.20.
- PHP 8.1 < 8.1.29.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. Las versiones de PHP 8.0, PHP 7 y PHP 5 están fuera de soporte y ya no reciben actualizaciones de seguridad. Sin embargo, el equipo oficial de PHP, lanzaron un parche de seguridad el 6 de junio del 2024.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/hackers-use-php-exploit-to-backdoor-windows-systems-with-new-malware/ • hxxps://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°194	Fecha: 22-08-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de inyección SQL en la API REST de Cisco Identity Services Engine		
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 una vulnerabilidad de severidad **MEDIA** de tipo inyección SQL en la API REST de Cisco Identity Services Engine (ISE). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado realice ataques de inyección SQL a ciegas.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-20417 de tipo inyección SQL en la API REST de Cisco ISE, podría permitir que un atacante remoto autenticado realice ataques de inyección SQL a ciegas.

Esta vulnerabilidad se debe a una validación insuficiente de la información proporcionada por el usuario en las llamadas a la API REST. Un atacante podría aprovechar esta vulnerabilidad al enviar información manipulada a un dispositivo afectado. Si lo hiciera, podría permitirle al atacante ver o modificar datos en el dispositivo afectado.

A. Productos afectados:

- Cisco Identity Services Engine, versión 3.4 y anteriores, 3.1, 3.2, 3.3.

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-ise-rest-5bPKrNtZ

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°194	Fecha: 22-08-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica 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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo confusión de tipos en el motor JavaScript V8 WebAssembly de Google Chrome. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario o la manipulación de datos.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-7971 de tipo confusión de tipos en V8 de Google Chrome, podría permitir a un atacante remoto explotar la corrupción del montón a través de una página HTML creada a medida. Esta vulnerabilidad podría permitir a un atacante remoto explotar la corrupción del montón, lo que podría llevar a la ejecución de código arbitrario o la manipulación de datos. El impacto se considera alto, ya que afecta al motor de JavaScript V8, un componente crítico de Google Chrome.

La explotación exitosa de esta vulnerabilidad podría comprometer la integridad y seguridad del navegador, exponiendo potencialmente los datos del usuario o permitiendo que un atacante obtenga el control del sistema afectado. Se requiere la interacción del usuario, pero puede explotarse a través de la red sin privilegios, lo que podría afectar la confidencialidad, la integridad y la disponibilidad.

A. Productos afectados:

- Esta vulnerabilidad afecta a la V8 de Google Chrome anterior a la versión 128.0.6613.84.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 128.0.6613.84 (Linux) 128.0.6613.84/.85 (Windows, Mac) que contiene una serie de correcciones y mejoras.
- Habilitar las actualizaciones automáticas de Google Chrome para garantizar la aplicación oportuna de parches de seguridad.
- Implementar la segmentación de la red y restringir el acceso a sitios web no confiables.
- Utilizar tecnologías de aislamiento del navegador para contener posibles vulnerabilidades.
- Concientizar a los usuarios sobre los riesgos de visitar sitios web no confiables o abrir contenido HTML sospechoso.

Fuente de Información:	• https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html • hxxps://cve.org/CVERecord?id=CVE-2024-7971

Índice alfabético