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

220-2024-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

El nuevo malware PondRAT oculto en paquetes Python ataca a desarrolladores de software 4
Múltiples vulnerabilidades en productos ESET 5
Vulnerabilidad de denegación de servicio en Apache Tomcat 6
Vulnerabilidad de severidad crítica en la herramienta pgAdmin 4 7
Índice alfabético 8

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°220	Fecha: 23-09-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El nuevo malware PondRAT oculto en paquetes Python ataca a desarrolladores de software		
Tipo de Ataque	Backdoors	Abreviatur	Backdoors
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Según nuevos hallazgos de la Unidad 42 de Palo Alto Networks, se ha observado que actores de amenazas utilizan paquetes Python envenenados como una forma de distribuir un nuevo malware llamado PondRAT como parte de una campaña en curso.

Este malware es una puerta trasera de macOS conocida que anteriormente se atribuyó al Grupo Lazarus y se implementó en ataques relacionados con la vulneración de la cadena de suministro de 3CX el año pasado.

2. DETALLES:

Esto es parte de una campaña de ciberataques persistente denominada Operación Dream Job, en la que se atrae a posibles objetivos con tentadoras ofertas de trabajo en un intento de engañarlos para que descarguen malware.

"Los atacantes cargaron varios paquetes de Python envenenados en PyPI, un repositorio popular de paquetes de Python de código abierto", dijo el investigador de la Unidad 42, Yoav Zemah, vinculando la actividad con moderada confianza a un actor de amenazas llamado Gleaming Pisces.

Se cree que el objetivo final de los ataques es "asegurar el acceso a los proveedores de la cadena de suministro a través de los puntos finales de los desarrolladores y, posteriormente, obtener acceso a los puntos finales de los clientes de los proveedores, como se observó en incidentes anteriores".

La lista de paquetes maliciosos, ahora eliminados del repositorio PyPI, se encuentra a continuación:

- real-ids (893 downloads)
- coloredtxt (381 downloads)
- beautifultext (736 downloads)
- minisound (416 downloads)

La cadena de infección es bastante simple en el sentido de que los paquetes, una vez descargados e instalados en los sistemas de los desarrolladores, están diseñados para ejecutar una siguiente etapa codificada que, a su vez, ejecuta las versiones para Linux y macOS del malware RAT después de recuperarlas de un servidor remoto.

PondRAT, una versión más sencilla de POOLRAT, viene con capacidades para cargar y descargar archivos, pausar operaciones durante un intervalo de tiempo predefinido y ejecutar comandos arbitrarios.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados, ni descargar adjuntos de correos desconocidos.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que pueda ayudar a detectar y bloquear descargas y sitios maliciosos, así como también habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Informar los intentos de phishing a sus equipos de TI y seguridad cuando corresponda.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/09/new-pondrat-malware-hidden-in-python.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°220	Fecha: 23-09-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos ESET		
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:

ESET ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo escalada de privilegios locales en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local escalar privilegios y generar una condición de denegación de servicio (DoS) en los sistemas afectados.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-6654 de tipo escalada de privilegios locales en productos ESET para macOS, podría permitir que un usuario conectado al sistema realice un ataque de DoS, que podría utilizarse indebidamente para desactivar la protección del producto de seguridad de ESET y provocar una ralentización general del sistema. ESET preparó y lanzó productos corregidos para que sus usuarios los descarguen e instalen.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-7400 de tipo escalada de privilegios locales, podría permitir a un atacante hacer un uso indebido de las operaciones de archivos de ESET durante la eliminación de un archivo detectado en el sistema operativo Windows para eliminar archivos sin tener los permisos adecuados para hacerlo.

La vulnerabilidad en el manejo de operaciones de archivos durante la eliminación de un archivo detectado potencialmente permitía a un atacante con capacidad para ejecutar código con pocos privilegios en el sistema de destino eliminar archivos arbitrarios, aumentando así sus privilegios.

A. Productos afectados:

- Versiones de ESET Cyber Security anteriores a la 7.5.74.0.
- ESET Endpoint Antivirus sin parche de seguridad del módulo Cleaner 1251.
- ESET Endpoint Security sin parche de seguridad del módulo Cleaner 1251 para Windows.
- Versiones de ESET Endpoint Security anteriores a 8.0.7200.0 para macOS.
- ESET File Security sin parche de seguridad del módulo Cleaner 1251 para Microsoft Azure.
- ESET Internet Security sin parche de seguridad del módulo Cleaner 1251.
- Parche de seguridad ESET Mail Security sin módulo Cleaner 1251 para Microsoft Exchange Server e IBM Domino.
- ESET NOD32 Antivirus sin parche de seguridad del módulo Cleaner 1251.
- ESET Safe Server sin parche de seguridad del módulo Cleaner 1251.
- ESET Security without Cleaner módulo 1251 parche de seguridad para Microsoft SharePoint Server.
- ESET Security Ultimate sin parche de seguridad del módulo Cleaner 1251.
- ESET Server Security sin parche de seguridad del módulo Cleaner 1251 para Windows Server.
- Parche de seguridad ESET Small Business Security sin módulo Cleaner 1251.
- ESET Smart Security Premium sin parche de seguridad del módulo Cleaner 1251.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible.

Fuente de Información:	• hxxps://support.eset.com/en/ca8725-local-privilege-escalation-vulnerability-in-eset-products-for-macos-fixed • hxxps://support.eset.com/en/ca8726-local-privilege-escalation-fixed-for-vulnerability-during-detected-file-removal-in-eset-products-for-windows

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°220	Fecha: 23-09-2024
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de denegación de servicio en Apache Tomcat		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **ALTA** de tipo agotamiento de los recursos en Apache Tomcat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

Apache Tomcat (Tomcat) es una implementación libre y de código abierto de las tecnologías Jakarta Servlet, Jakarta Expression Language y WebSocket. Proporciona un entorno de servidor web HTTP "Java puro" en el que también se puede ejecutar código Java. Por lo tanto, es un servidor de aplicaciones web Java, aunque no un servidor de aplicaciones JEE completo. Tomcat es desarrollado y mantenido por una comunidad abierta de desarrolladores bajo los auspicios de la Apache Software Foundation, publicado bajo la licencia Apache License 2.0.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-38286 de tipo agotamiento de los recursos en Apache Tomcat, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a que la aplicación no controla adecuadamente el consumo de recursos internos durante el proceso de enlace TLS. Un atacante remoto puede iniciar múltiples conexiones TLS, provocar el agotamiento de la memoria y realizar un ataque de DoS. Para explotar esta vulnerabilidad, un atacante tendría que enviar una solicitud especialmente diseñada a la aplicación afectada.

Tomcat, bajo ciertas configuraciones en cualquier plataforma, permite a un atacante provocar un OutOfMemoryError al abusar del proceso de protocolo de enlace TLS.

A. Productos afectados:

- Apache Tomcat 11.0.0-M1 a 11.0.0-M20.
- Apache Tomcat 10.1.0-M1 a 10.1.24.
- Apache Tomcat 9.0.13 a 9.0.89.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://lists.apache.org/thread/bk6k97ps0mcdw7nv6c1rpoyh8kn9cj93

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°220	Fecha: 23-09-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la herramienta pgAdmin 4		
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 una vulnerabilidad de severidad **CRÍTICA** de tipo credenciales insuficientemente protegidas en múltiples versiones en la herramienta pgAdmin 4 que afecta a un bloque de código desconocido del componente OAuth2 Authentication Handler. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener el ID y el secreto del cliente OAuth2, lo que lleva a un acceso no autorizado a los datos del usuario.

2. DETALLES:

pgAdmin es una potente herramienta de desarrollo y administración de código abierto para PostgreSQL, ampliamente reconocida por su interfaz fácil de usar y su sólido conjunto de funciones. Funciona como una interfaz gráfica que simplifica la gestión de bases de datos PostgreSQL, haciéndola accesible tanto para principiantes como para usuarios avanzados.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-9014 de tipo credenciales insuficientemente protegidas en múltiples versiones de la herramienta pgAdmin, podría permitir a un atacante obtener acceso no autorizado a los datos de los usuarios mediante la explotación de fallas de autenticación de OAuth2.

Esta vulnerabilidad permite que un atacante obtenga potencialmente el ID y secreto del cliente, lo que lleva a un acceso no autorizado a los datos del usuario.

A. Productos afectados:

- Esta vulnerabilidad afecta a las versiones 8.11 y anteriores de pgAdmin.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 8.12 que mitiga esta vulnerabilidad.
- Asimismo, si la actualización no es posible de inmediato, considerar deshabilitar la autenticación OAuth2 temporalmente si es factible.
- Implementar una segmentación de red sólida para limitar el acceso a las instancias de pgAdmin.
- Monitorear cualquier actividad sospechosa relacionada con la autenticación OAuth2 en pgAdmin.
- Auditar y rotar regularmente los ID y secreto del cliente OAuth2.
- Implementar capas de autenticación adicionales cuando sea posible.

Fuente de Información:	• hxxps://github.com/pgadmin-org/pgadmin4/issues/7945 • hxxps://www.postgresql.org/about/news/pgadmin-4-v812-released-2937/

Índice alfabético

Backdoors 4
Explotación de vulnerabilidades conocidas 5, 6, 7