PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 26 de marzo de 2024

074-2024-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 Aérea del 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 las empresas 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

Las aplicaciones VPN gratuitas en Google Play convirtieron los teléfonos Android en servidores proxy 4
Múltiples vulnerabilidades en GNU Emacs 6
Múltiples vulnerabilidades en IBM WebSphere Service Registry and Repository 7
Vulnerabilidad de inyección SQL en el paquete pgproto3 8
Vulnerabilidad de DoS en la versión de Microsoft del conjunto de herramientas Go 9
Índice alfabético 10

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°074	Fecha: 26-03-2024
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Las aplicaciones VPN gratuitas en Google Play convirtieron los teléfonos Android en servidores proxy		
Tipo de Ataque	Intentos reiterativos de acceso a recursos	Abreviatura	IntReiAccRec
Medios de propagación	Red, Internet		
Código de familia	A	Código de Sub familia	A01
Clasificación temática familia	Acceso no autorizado		

Descripción

1. ANTECEDENTES:

Se encontraron más de 15 aplicaciones VPN gratuitas en Google Play utilizando un kit de desarrollo de software malicioso que convertía los dispositivos Android en servidores proxy residenciales involuntarios, probablemente utilizados para delitos cibernéticos y robots de compras.

2. DETALLES:

Los proxies residenciales son dispositivos que dirigen el tráfico de Internet a través de dispositivos ubicados en hogares para otros usuarios remotos, haciendo que el tráfico parezca legítimo y con menos probabilidades de ser bloqueado.

Si bien tienen usos legítimos para la investigación de mercado, la verificación de anuncios y el SEO, muchos ciberdelincuentes los utilizan para ocultar actividades maliciosas , incluido el fraude publicitario, el spam, el phishing, el relleno de credenciales y la pulverización de contraseñas.

Los usuarios pueden registrarse voluntariamente en servicios de proxy para obtener recompensas monetarias o de otro tipo a cambio, pero algunos de estos servicios de proxy emplean medios poco éticos y turbios para instalar sus herramientas de proxy en los dispositivos de las personas en secreto.

Cuando se instala en secreto, las víctimas verán secuestrado su ancho de banda de Internet sin su conocimiento y correrán el riesgo de tener problemas legales por aparecer como fuente de actividad maliciosa.

Un informe publicado por el equipo de inteligencia de amenazas Satori de HUMAN enumera 28 aplicaciones en Google Play que secretamente convirtieron dispositivos Android en servidores proxy. De estas 28 aplicaciones, 17 se hicieron pasar como software VPN gratuito.

Los analistas de Satori informan que todas las aplicaciones infractoras utilizaban un kit de desarrollo de software (SDK) de LumiApps que contenía " Proxylib ", una biblioteca de Golang para realizar el proxy.

HUMAN descubrió la primera aplicación de operador PROXYLIB en mayo de 2023, una aplicación VPN gratuita para Android llamada "Oko VPN". Más tarde, los investigadores encontraron la misma biblioteca utilizada por el servicio de monetización de aplicaciones LumiApps para Android.

Una investigación posterior reveló un conjunto de 28 aplicaciones que utilizaban la biblioteca ProxyLib para convertir dispositivos Android en servidores proxy, que se enumeran a continuación:

- VPN sencilla
- Teclado de animaciones
- Paso de fuego
- VPN de hoja de bytes
- Lanzador de Android 12 (por CaptainDroid)
- Lanzador de Android 13 (por CaptainDroid)
- Lanzador de Android 14 (por CaptainDroid)
- Feeds de CaptainDroid
- Películas clásicas antiguas gratuitas (por CaptainDroid)
- Comparación de teléfonos (por CaptainDroid)

- VPN de vuelo rápido
- VPN rápida de Fox
- VPN de línea rápida
- Animación divertida de Char Ging
- Bordes de limusina
- OkoVPN
- Lanzador de aplicaciones de teléfono
- VPN de flujo rápido
- VPN de muestra
- Trueno seguro
- Brilla Seguro
- Surf de velocidad
- VPN de escudo rápido
- VPN de pista turbo
- VPN de túnel turbo
- VPN de destello amarillo
- VPN ultra
- Ejecutar VPN

LumiApps es una plataforma de monetización de aplicaciones de Android que afirma que su SDK utilizará la dirección IP de un dispositivo para cargar páginas web en segundo plano y enviar los datos recuperados a las empresas.

no está claro si los desarrolladores de aplicaciones gratuitas sabían que el SDK estaba convirtiendo los dispositivos de sus usuarios en servidores proxy que podrían usarse para actividades no deseadas.

Tras el informe de HUMAN, Google eliminó todas las aplicaciones nuevas y restantes que utilizaban el SDK de LumiApps de Play Store en febrero de 2024 y actualizó Google Play Protect para detectar las bibliotecas de LumiApps utilizadas en las aplicaciones.

Mientras tanto, muchas de las aplicaciones enumeradas anteriormente ahora están disponibles nuevamente en la tienda Google Play, presumiblemente después de que sus desarrolladores eliminaron el SDK infractor. A veces se publicaban desde diferentes cuentas de desarrollador, lo que podría indicar prohibiciones de cuentas anteriores.

3. RECOMENDACIONES:

- Eliminar por completo las aplicaciones listadas anteriormente.
- Utilizar aplicaciones VPN de pago en lugar de servicios gratuitos.
- Utilizar una solución de seguridad para dispositivos móviles que sea confiable para bloquear y remover amenazas.
- Confiar únicamente en apps cuyo enlace se encuentre en el sitio oficial del servicio.
- Mantener el software del dispositivo actualizado.
- Verificar los permisos que solicitan las aplicaciones al momento de instalarlas: si piden permisos innecesarios, puede ser indicio de una intención sospechosa.
- Revisar los comentarios, valoraciones, cantidad de descargas, y quién es el desarrollador de la app que se desea descargar desde Google Play.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/free-vpn-apps-on-google-play-turned-android-phones-into-proxies/ • hxxps://www.welivesecurity.com/es/seguridad-moviles/me-puedo-infectar-descargando-aplicacion-google-play/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°074**	**Fecha: 26-03-2024**
		Página: 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en GNU Emacs.		
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 **ALTA** de tipo verificación insuficiente de la autenticidad de los datos y uso de una función potencialmente peligrosa en GNU Emacs. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30205 de tipo verificación insuficiente de la autenticidad de los datos, existe debido a que Emacs en modo Org considera que el contenido de archivos remotos es confiable. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30202 de tipo uso de una función potencialmente peligrosa, existe debido al uso de métodos peligrosos al procesar archivos que no son de confianza. Un atacante remoto puede engañar a la víctima para que abra un documento especialmente diseñado y ejecute código Lisp arbitrario como parte de activar el modo Org.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30203 de tipo verificación insuficiente de la autenticidad de los datos, existe debido a que Gnus trata el contenido MIME en línea como confiable. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30204 de tipo verificación insuficiente de la autenticidad de los datos, existe debido a que la vista previa de LaTeX está habilitada de forma predeterminada para los archivos adjuntos de correo electrónico. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario en el sistema.

A. Productos afectados:

- Emacs: 29.0.90 - 29.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°074**	**Fecha: 26-03-2024**
		Página: 7 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en IBM WebSphere Service Registry and Repository		
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 **ALTA** y **MEDIA** de tipo limitación inadecuada de un nombre de ruta a un directorio restringido (Path Traversal), deserialización de datos que no son de confianza, escritura fuera de límites, desbordamiento de búfer basado en la pila y agotamiento de recursos en IBM WebSphere Service Registry and Repository. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto eludir la autenticación, ejecutar código arbitrario en el sistema de destino y realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-34478 de tipo recorrido de camino, existe debido a un error de validación de entrada al procesar secuencias de recorrido de directorio. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y omitir el proceso de autenticación, cuando se usa junto con API u otros marcos web que enrutan solicitudes basadas en solicitudes no normalizadas.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-1471 de tipo deserialización de datos que no son de confianza, existe debido a una validación de entrada insegura al procesar datos serializados dentro de la clase Constructor() de SnakeYaml. Un atacante remoto puede pasar contenido yaml especialmente diseñado a la aplicación y ejecutar código arbitrario en el sistema de destino.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad **media**: CVE-2022-41854, CVE-2022-38752, CVE-2022-38751, CVE-2022-38750, CVE-2022-38749 y CVE-2022-25857.

A. Productos afectados:

- WebSphere Service Registry and Repository: todas las versiones.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7129833

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°074	Fecha: 26-03-2024
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de inyección SQL en el paquete pgproto3		
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 neutralización inadecuada de elementos especiales utilizados en un comando SQL (Inyección SQL) en el paquete pgproto3. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos.

2. DETALLES:

PGProto3 es una especificación del protocolo de comunicación utilizada en la industria de la tecnología, especialmente en el ámbito de las bases de datos. En particular, se asocia comúnmente con PostgreSQL, un sistema de gestión de bases de datos relacional de código abierto muy popular.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-27304 de tipo inyección SQL, existe debido a una limpieza insuficiente de los datos proporcionados por el usuario al manejar consultas demasiado grandes que superan los 4 GB de tamaño. Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

A. Productos afectados:

- PostgreSQL driver and toolkit for Go: 4.0.0 - 5.5.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://github.com/jackc/pgx/security/advisories/GHSA-mrww-27vc-gghv • hxxp://github.com/jackc/pgproto3/security/advisories/GHSA-7jwh-3vrq-q3m8 • hxxp://github.com/jackc/pgproto3/commit/945c2126f6db8f3bea7eeebe307c01fe92bca007 • hxxp://github.com/jackc/pgx/commit/adbb38f298c76e283ffc7c7a3f571036fea47fd4 • hxxp://github.com/jackc/pgx/commit/c543134753a0c5d22881c12404025724cb05ffd8 • hxxp://github.com/jackc/pgx/commit/f94eb0e2f96782042c96801b5ac448f44f0a81df

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°074	Fecha: 26-03-2024
		Página: 9 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de DoS en la versión de Microsoft del conjunto de herramientas Go		
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 **MEDIA** de tipo falta de liberación de memoria después de la vida útil en la versión de Microsoft del conjunto de herramientas Go. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS) en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-1394 de falta de liberación de memoria después de la vida útil, existe debido a una pérdida de memoria en el código de cifrado/descifrado RSA al manejar entradas que no son de confianza. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y realizar un ataque de denegación de servicio.

A. Productos afectados:

- go: 1.4.0-1 - 1.22.1-1.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://bugzilla.redhat.com/show_bug.cgi?id=2262921 • hxxp://github.com/golang-fips/openssl/security/advisories/GHSA-78hx-gp6g-7mj6

Índice alfabético

Explotación de vulnerabilidades conocidas 6, 7, 8, 9
Intentos reiterativos de acceso a recursos 4