multisoft
Soluciones en Movimiento

NEWS

TLP:CLEAR

# NOTICIAS DE CIBER SEGURIDAD

05 de julio 2024

multisoft
Soluciones en Movimiento

News

Multisoft Soluciones en Movimiento
Multisoft S.A.S
@Multisoft_SAS

# Introducción

**El equipo del SOC-Multisoft presenta en este documento un listado de las noticias más relevantes de la última semana.** Estas noticias son insumos clave para asegurar los activos e información de nuestros clientes, al hacer referencia a amenazas y vulnerabilidades.


PBX: +57 601 329 97 99
Avenida 15 No. 100-69 Piso 7
Bogotá D.C - Colombia
www.multisoft.com.co

PPBX: (506) 411 1860
Centro corporativo Escazú Village
Torre 1 Piso 2 San José - Costa Rica
www.multisoft.com.cr

# VULNERABILIDADES

## Juniper Networks lanza una actualización de seguridad crítica para enrutadores

Criticidad: **Alta**

La vulnerabilidad, rastreada como CVE-2024-2973 es una omisión de autenticación mediante una ruta o canal alternativo en el enrutador inteligente de sesión de Juniper Networks o Conductor que se ejecuta con un par redundante permite a un atacante basado en la red eludir la autenticación y tomar el control total del dispositivo; Juniper Networks ha lanzado actualizaciones de seguridad fuera de banda para abordar una falla de seguridad crítica que podría conducir a una omisión de autenticación en algunos de sus enrutadores. La lista de dispositivos afectados se enumera a continuación: Session Smart Router (todas las versiones anteriores a la 5.6.15, desde la 6.0 anterior a la 6.1.9-lts y desde la 6.2 anterior a la 6.2.5-sts), Session Smart Conductor (todas las versiones anteriores a la 5.6.15, desde la 6.0 anterior a la 6.1.9-lts y desde la 6.2 anterior a la 6.2.5-sts) Enrutador de garantía WAN (versiones 6.0 anteriores a 6.1.9-lts y 6.2 versiones anteriores a 6.2.5-sts).

Referencia: https://thehackernews.com/2024/07/juniper-networks-releases-critical.html

## Vulnerabilidad de OpenSSH podría llevar a RCE como root en sistemas Linux

Criticidad: **Alta**

La vulnerabilidad, cuyo nombre en clave es regreSSHion, se le ha asignado el identificador CVE CVE-2024-6387. Reside en el componente de servidor OpenSSH, que está diseñado para escuchar las conexiones de cualquiera de las aplicaciones cliente. La vulnerabilidad permite la ejecución remota de código (RCE) no autenticada como root en sistemas Linux basados en glibc. La firma de ciberseguridad dijo que identificó no menos de 14 millones de instancias de servidor OpenSSH potencialmente vulnerables expuestas a Internet, y agregó que es una regresión de una falla ya parcheada de 18 años de antigüedad rastreada como CVE-2006-5051, con el problema restablecido en octubre de 2020 como parte de la versión 8.5p1 de OpenSSH.

Referencia: https://thehackernews.com/2024/07/new-openssh-vulnerability-could-lead-to.html

## Se aprovecha una falla de MSHTML de Microsoft para distribuir la herramienta espía MerkSpy

Criticidad: **Alta**

Se ha observado que actores de amenazas desconocidos explotan una falla de seguridad ahora parcheada en Microsoft MSHTML para entregar una herramienta de vigilancia llamada MerkSpy como parte de una campaña dirigida principalmente a usuarios en Canadá, India, Polonia y los EE. UU.
"MerkSpy está diseñado para monitorear clandestinamente las actividades de los usuarios, capturar información confidencial y establecer persistencia en sistemas comprometidos", dijo la investigadora de Fortinet FortiGuard Labs, Cara Lin , en un informe publicado la semana pasada.
El punto de partida de la cadena de ataque es un documento de Microsoft Word que aparentemente contiene una descripción del puesto de ingeniero de software.

Referencia: https://thehackernews.com/2024/07/microsoft-mshtml-flaw-exploited-to.html

## Las fallas críticas en los CocoaPods exponen las aplicaciones de iOS y macOS a ataques a la cadena de suministro

Criticidad: **Media**

Se ha descubierto un trío de fallas de seguridad en el administrador de dependencias de CocoaPods para los proyectos Swift y Objective-C Cocoa que podrían explotarse para organizar ataques a la cadena de suministro de software, Una de las vulnerabilidades es CVE-2024-38368 (puntuación CVSS: 9,3), que hace posible que un atacante abuse del proceso "Claim Your Pods" y tome el control de un paquete, lo que le permite manipular el código fuente e introducir cambios maliciosos. El segundo error es aún más crítico (CVE-2024-38366, puntuación CVSS: 10.0) y aprovecha un flujo de trabajo de verificación de correo electrónico inseguro para ejecutar código arbitrario en el servidor troncal.

Referencia: https://thehackernews.com/2024/07/critical-flaws-in-cocoapods-expose-ios.html

## RegreSSHion: vulnerabilidad de RCE en OpenSSH afecta a 700.000 sistemas Linux

Criticidad: **Media**

La Unidad de Investigación de Amenazas de Qualys ha identificado una vulnerabilidad recientemente descubierta en OpenSSH, denominada “regreSSHion” (CVE-2024-6387). Esta falla crítica, que permite la ejecución remota de código (RCE) no autenticada como root, afecta a más de 700.000 sistemas Linux expuestos a Internet. La vulnerabilidad regreSSHion es una condición de carrera del controlador de señales en el servidor de OpenSSH (sshd) que puede explotarse para ejecutar código arbitrario con los privilegios más altos.

Referencia: https://gbhackers.com/regresshion-rce-flaw/

## Vulnerabilidad de inyección de comandos de día cero en Cisco NX-OS permitió a los piratas informáticos obtener acceso a la raíz

Criticidad: **Media**

Cisco ha revelado una vulnerabilidad crítica en su sistema operativo de red ampliamente utilizado NX-OS que podría permitir a los atacantes ejecutar comandos arbitrarios con privilegios de root en los dispositivos afectados. La compañía insta a los clientes a actualizar a versiones parcheadas lo antes posible. La vulnerabilidad identificada como CVE-2024-20399 existe en la interfaz de línea de comandos (CLI) de NX-OS debido a una validación insuficiente de los argumentos pasados a comandos de configuración específicos.

Referencia: https://gbhackers.com/cisco-nx-os-zero-day-command-injection-vulnerability/

## Nueva vulnerabilidad en CPU Intel, 'Indirector', expone datos confidenciales

Criticidad: **Media**

Las CPU modernas de Intel, incluidas Raptor Lake y Alder Lake, han sido encontradas vulnerables a un nuevo ataque de canal lateral que podría ser explotado para filtrar información confidencial de los procesadores. El ataque, cuyo nombre en código es Indirector por los investigadores de seguridad Luyi Li, Hosein Yavarzadeh y Dean Tullsen, aprovecha las deficiencias identificadas en Indirect Branch Predictor (IBP) y Branch Target Buffer (BTB) para eludir las defensas existentes y comprometer la seguridad de las CPU. "El Predictor de Rama Indirecta (IBP) es un componente de hardware en las CPU modernas que predice las direcciones de destino de las ramas indirectas", señalaron los investigadores .

Referencia: https://thehackernews.com/2024/07/new-intel-cpu-vulnerability-indirector.html

## Un fallo crítico en un complemento de WordPress expone más de 90.000 sitios de WordPress

Criticidad: **Media**

Se ha descubierto una vulnerabilidad crítica en el popular complemento de WordPress “Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress WooCommerce”. A la falla, identificada como CVE-2024-6172, se le ha asignado una puntuación CVSS de 9,8, lo que indica su grave impacto. La vulnerabilidad fue revelada públicamente el 1 de julio de 2024 y actualizada por última vez el 2 de julio de 2024 por el investigador conocido como shaman0x01 del equipo Shaman Red.

Referencia: https://gbhackers.com/critical-wordpress-plugin/

## Los piratas informáticos afirman que el Sandbox ha escapado de RCE en Google Chrome 0-DAY

Criticidad: **Media**

Un grupo de hackers afirmó haber descubierto una vulnerabilidad crítica de día cero en Google Chrome. Este exploit, que al parecer permite el escape de una zona protegida y la ejecución remota de código (RCE), podría comprometer potencialmente a millones de usuarios en todo el mundo. Según lo descrito por los hackers, la vulnerabilidad de día cero permite un escape de sandbox, una técnica que permite que el código malicioso salga del entorno aislado diseñado para contenerlo.

Referencia: https://gbhackers.com/claiming-sandboxrce-0-day/

## TeamViewer detecta una brecha de seguridad en el entorno de TI corporativo

Criticidad: **Media**

TeamViewer reveló el jueves que detectó una "irregularidad" en su entorno de TI corporativo interno el 26 de junio de 2024.
"Activamos inmediatamente nuestro equipo de respuesta y procedimientos, iniciamos investigaciones junto con un equipo de expertos en seguridad cibernética de renombre mundial e implementamos las medidas de remediación necesarias", dijo la compañía en un comunicado.
Señaló además que su entorno de TI corporativo está completamente aislado del entorno del producto y que no hay evidencia que indique que los datos de los clientes se hayan visto afectados como resultado del incidente.
No reveló ningún detalle sobre quién pudo haber estado detrás de la intrusión y cómo pudieron lograrla, pero dijo que se está llevando a cabo una investigación y que proporcionaría actualizaciones sobre el estado a medida que haya nueva información disponible.

Referencia: https://thehackernews.com/2024/06/teamviewer-detects-security-breach-in.html

## Los piratas informáticos chinos aprovechan los ataques de día cero de los switches Cisco para distribuir malware

Criticidad: **Media**

Un grupo de ciberespionaje vinculado a China, llamado Velvet Ant, ha explotado una vulnerabilidad de día cero (CVE-2024-20399, puntuación CVSS: 6.0) en el software Cisco NX-OS. Esta falla permite a un atacante local autenticado ejecutar comandos arbitrarios como root en dispositivos afectados. Utilizando esta vulnerabilidad, Velvet Ant ha desplegado malware personalizado para acceder remotamente a conmutadores Cisco Nexus comprometidos, cargar archivos adicionales y ejecutar código. La vulnerabilidad se debe a una validación insuficiente de argumentos en comandos CLI de configuración, según la firma de ciberseguridad Sygnia.

Referencia: https://thehackernews.com/2024/07/chinese-hackers-exploiting-cisco.html

## La vulnerabilidad de Juniper SRX permite a los atacantes activar una condición de denegación de servicio

Criticidad: **Media**

Una vulnerabilidad en Junos OS en los dispositivos de la serie SRX permite a los atacantes desencadenar un ataque DoS mediante el envío de tráfico válido diseñado, lo que es causado por un manejo inadecuado de condiciones excepcionales dentro del motor de reenvío de paquetes (PFE) y provoca fallas y reinicios del PFE al recibir el tráfico específico. Un atacante puede aprovechar esto enviando continuamente tráfico malicioso, lo que provoca una condición de denegación de servicio sostenida y potencialmente afecta la disponibilidad de los recursos de la red.

Referencia: https://gbhackers.com/juniper-srx-dos-vulnerability/

## Las vulnerabilidades de GoG permiten a los atacantes piratear instancias y robar el código fuente

Criticidad: **Media**

Gogs es un sistema de alojamiento de código abierto estándar utilizado por muchos desarrolladores. Los investigadores de ciberseguridad de SonarSource han descubierto recientemente varias vulnerabilidades de Gogs. El servidor SSH integrado de Gogs contiene una vulnerabilidad de inyección de argumentos que permite a atacantes autenticados ejecutar cualquier comando en el servidor.
La vulnerabilidad explota la opción ' –split-string ' en el comando 'env' para eludir las medidas de seguridad.
Como resultado, esta vulnerabilidad continúa sin parchearse incluso en la última versión de Gogs (0.13.0).

Referencia: https://gbhackers.com/gogs-vulnerabilities-hack-steal-source-code/

## Se duplican los ciberataques con exploits contra usuarios de Linux

Criticidad: **Media**

Según un reciente informe de Kaspersky, 'Exploits and vulnerabilities in Q1 2024', el número de ataques a través de exploits experimentó un notable incremento a finales de 2023 en comparación con el inicio del último año, destacando una tendencia preocupante que, si bien ha mostrado un ligero descenso en 2024, continúa siendo significativa debido a la creciente adopción de los sistemas operativos Linux. Este aumento en la actividad maliciosa coincide con un alarmante crecimiento en las vulnerabilidades críticas, que se triplicaron en 2023 respecto al promedio observado entre 2019 y 2022.

Referencia: https://cybersecuritynews.es/se-duplican-los-ciberataques-con-exploits-contra-usuarios-de-linux/

## Vulnerabilidad de inyección de comandos de la CLI del software Cisco NX-OS

Criticidad: **Media**

Una vulnerabilidad en la CLI del software Cisco NX-OS podría permitir que un usuario autenticado en posesión de credenciales de administrador ejecute comandos arbitrarios como root en el sistema operativo subyacente de un dispositivo afectado.

Referencia:https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP?vs_f=Cisco%20Security%20Advisory=Security%20Intelligence=RSS=Cisco%20NX-OS%20Software%20CLI%20Command%20Injection%20Vulnerability=1

# MALWARE

## Kimsuky usa la extensión TRANSLATEXT de Chrome para robar datos confidenciales

Criticidad: **Alta**

El actor de amenazas vinculado a Corea del Norte conocido como Kimsuky ha sido vinculado al uso de una nueva extensión maliciosa de Google Chrome que está diseñada para robar información confidencial como parte de un esfuerzo continuo de recopilación de inteligencia

Referencia: https://thehackernews.com/2024/06/kimsuky-using-translatext-chrome.html

## Hackean los productos de una empresa de software india para propagar malware que roba datos

Criticidad: **Media**

Los instaladores de tres productos de software de la empresa Conceptworld han sido comprometidos para distribuir malware. Según Rapid7, estos instaladores manipulados de Notezilla, RecentX y Copywhiz ejecutan malware diseñado para robar credenciales de navegadores y billeteras de criptomonedas, registrar el portapapeles y pulsaciones de teclas, y descargar nuevas cargas útiles en sistemas Windows infectados. El malware también establece persistencia mediante tareas programadas y establece conexiones con un servidor de comando y control para robar datos y recibir órdenes adicionales.

Referencia: https://thehackernews.com/2024/07/indian-software-firms-products-hacked.html

## El software espía CapraRAT disfrazado de aplicaciones populares amenaza a los usuarios de Android

Criticidad: **Media**

El grupo de amenazas Transparent Tribe ha continuado su campaña maliciosa lanzando aplicaciones de Android con malware, enfocándose en usuarios específicos como jugadores móviles, entusiastas de las armas y seguidores de TikTok. Estas aplicaciones, como "Juego loco", "Videos Sexys", "TikToks" y "Armas", contienen spyware que utiliza WebView para redirigir a los usuarios a sitios web maliciosos mientras accede de manera clandestina a datos sensibles como ubicaciones, mensajes SMS, contactos y registros de llamadas. Una evolución del malware es que ahora evita solicitar ciertos permisos, indicando un cambio hacia el uso del malware como herramienta de vigilancia en lugar de solo una puerta trasera.

Referencia: https://thehackernews.com/2024/07/caprarat-spyware-disguised-as-popular.html

## Los piratas informáticos utilizan Dropbox y Google Docs para distribuir el malware Orcinius

Criticidad: **Media**

Se ha descubierto un nuevo troyano Orcinius que utiliza VBA Stomping para ocultar su infección. El troyano de múltiples etapas utiliza Dropbox y Google Docs para mantenerse actualizado y entregar cargas útiles de segunda etapa. “El malware contiene una macro VBA ofuscada que se conecta a Windows para monitorear las ventanas en ejecución y las pulsaciones de teclas y crea persistencia utilizando claves de registro”, compartió el equipo de investigación de amenazas de SonicWall Capture Labs con Cyber Security News.

Referencia: https://gbhackers.com/hackers-dropbox-google-orcinius-malware/

## Backdoor Oyster se propaga a través de descargas de software troyanizado

Criticidad: **Media**

Una campaña de publicidad maliciosa está distribuyendo instaladores troyanizados de software popular como Google Chrome y Microsoft Teams para instalar una puerta trasera llamada Oyster. Según Rapid7, los usuarios son redirigidos a sitios web falsos que alojan cargas maliciosas al buscar software en motores de búsqueda como Google y Bing. Al intentar descargar el software, se inicia una cadena de infección que instala Oyster, permitiendo la recopilación de información del host comprometido, comunicación con una dirección de comando y control (C2) y ejecución remota de código.

Referencia: https://thehackernews.com/2024/06/oyster-backdoor-spreading-via.html

## El troyano bancario Mekotio amenaza los sistemas financieros de América Latina

Criticidad: **Media**

El troyano bancario Mekotio es un sofisticado malware que ha estado activo desde al menos 2015, dirigido principalmente a países de América Latina con el objetivo de robar información confidencial, en particular credenciales bancarias, de sus objetivos. Originario de la región latinoamericana, ha sido particularmente prolífico en Brasil, Chile, México, España y Perú. Además, Mekotio parece compartir un origen común con otros notables programas maliciosos bancarios latinoamericanos, como Grandoreiro, que fue interrumpido por las fuerzas del orden a principios de este año. Mekotio a menudo se entrega a través de correos electrónicos de phishing, empleando ingeniería social para engañar a los usuarios para que interactúen con enlaces o archivos adjuntos maliciosos.

Referencia: https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html