SECURESOFT CORPORATION

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

13 de Octubre de 2024

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Antifraude

ADWI-FOR-2023-002

Índice

1. Objetivo

El presente documento de inteligencia tiene como objetivo informar sobre las principales vulnerabilidades y amenazas que se han detectado en el ciberespacio.

2. Alcance

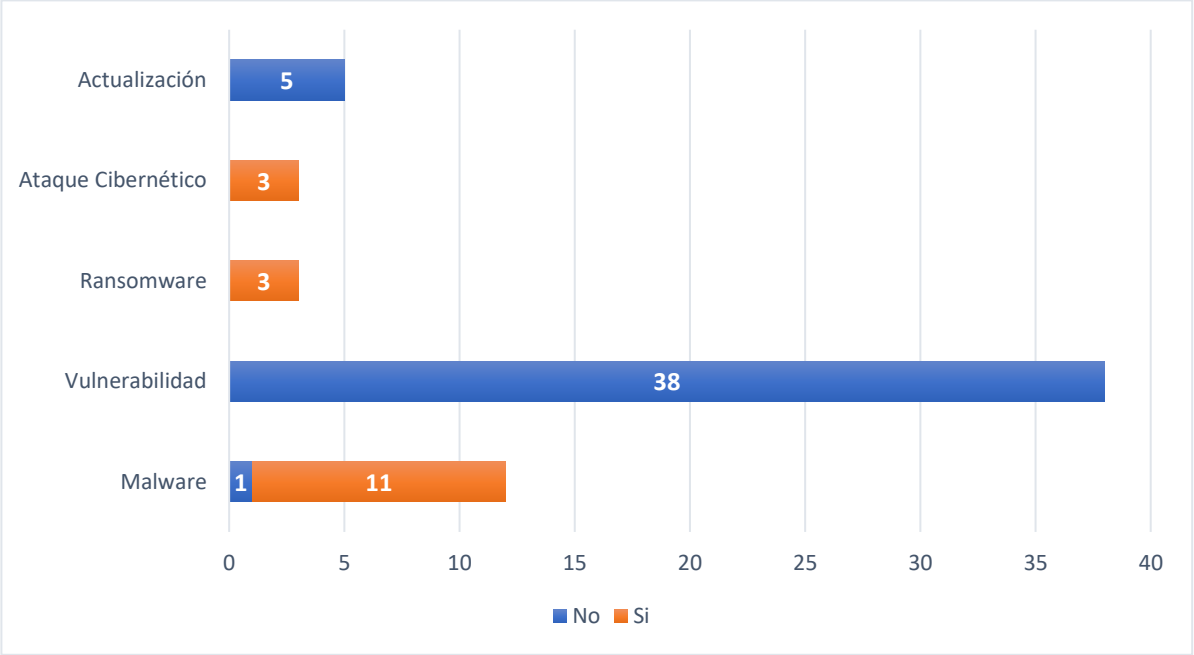
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 hasta el 30 de Setiembre del 2024.

3. Resumen

En el presente informe se exponen 61 análisis de vulnerabilidad y amenazas, de las cuales 30 tienen severidad alta, 29 severidad crítica y 2 severidad media.

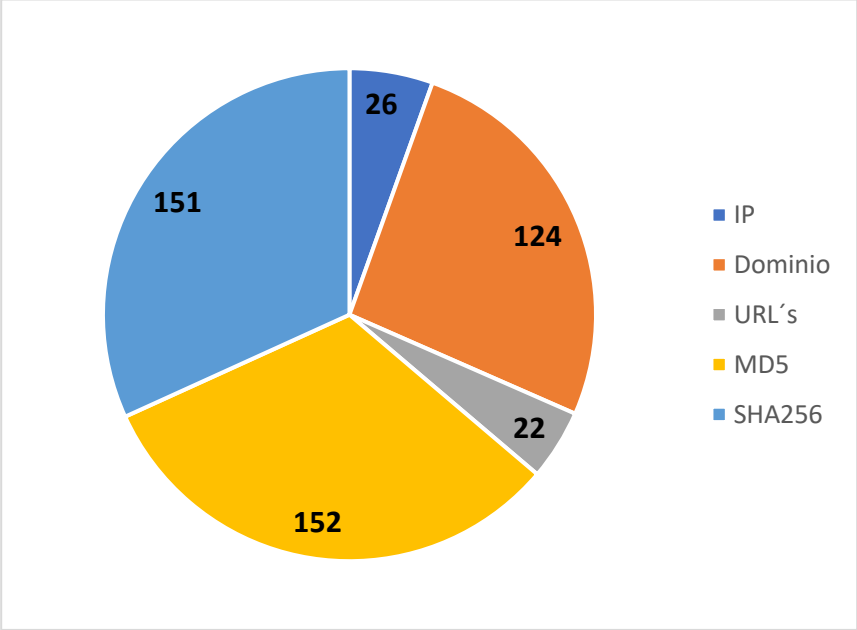
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron de actualización, ataque cibernético, vulnerabilidad, ransomware, malware entre otros. Los que se detallan a continuación, separándolas de acuerdo con si contaban con indicadores de compromiso (IoC) o no.



Indicadores de Compromiso (IoC)

En las investigaciones elaboradas para el presente informe, se han distribuido 475 IoC's entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Se ha identificado una vulnerabilidad recientemente descubierta en Spring Framework, que podría permitir a los atacantes acceder a cualquier archivo del sistema. Para más información leer el Boletín 2024-876.

- D-Link ha publicado soluciones para vulnerabilidades críticas en tres modelos populares de enrutadores inalámbricos que permiten a atacantes remotos ejecutar código arbitrario o acceder a los dispositivos utilizando credenciales codificadas. Para más información leer el Boletín 2024-878.

- Recientemente, se ha descubierto una importante vulnerabilidad de seguridad en AutoGPT, una potente herramienta de inteligencia artificial diseñada para automatizar tareas a través de agentes inteligentes. Para más información leer el Boletín 2024-880.

- Recientemente, se descubrió que más de 1,000 instancias empresariales de ServiceNow estaban exponiendo información sensible, como PII y credenciales, debido a configuraciones erróneas en los permisos de las bases de conocimientos. Para más información leer el Boletín 2024-882.

- Recientemente SolarWinds ha corregido dos fallas de vulnerabilidades en su software Access Rights Manager (ARM), la vulnerabilidad más crítica fue identificada con el CVE-2024-28991. Se debe a una falta de validación de los datos proporcionados por el usuario, exponiendo los dispositivos ARM a una vulnerabilidad de deserialización que podría ser abusada para ejecutar código arbitrario. Para más información leer el Boletín 2024-883.

- Recientemente han corregido una vulnerabilidad crítica en VMware vCenter Server (CVE-2024-38812) que permite la ejecución remota de código a través de un paquete de red, afectando a los productos vSphere y Cloud Foundation. La falla se debe a un desbordamiento de heap en el protocolo DCE/RPC de vCenter. Para más información leer el Boletín 2024-884.

- Recientemente, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) ha añadido cuatro fallos críticos de Adobe Flash Player a su catálogo de vulnerabilidades explotadas conocidas (KEV). Para más información leer el Boletín 2024-885.

- Recientemente Red Hat OpenShift, la plataforma de nube híbrida, se enfrenta a dos vulnerabilidades críticas que podrían afectar significativamente su postura de seguridad. Para más información leer el Boletín 2024-886.

- GitLab ha lanzado actualizaciones de seguridad para abordar una vulnerabilidad crítica de bypass en la autenticación e Security Assertion Markup Language (SAML), CVE-2024-45409, que afecta a las instalaciones autogestionadas de las ediciones Community y Enterprise. Esta falla, originada en las bibliotecas OmniAuth-SAML y Ruby-SAML, permite a un atacante

manipular respuestas SAML para eludir la autenticación, haciéndose pasar por usuarios autenticados. Para más información leer el Boletín 2024-888.

- Investigadores de seguridad anunciaron una nueva vulnerabilidad en Next.js estaría afectando a versiones específicas del marco, dejando implementaciones expuestas ante ciberataques de envenenamiento de caché. Para más información leer el Boletín 2024-889.

- El equipo de Chrome ha anunciado oficialmente el lanzamiento de Chrome 129, para Windows, Mac y Linux. Esta actualización, que se irá desplegando gradualmente a lo largo de los próximos días, soluciona varias vulnerabilidades de seguridad e introduce diversas mejoras. Para más información leer el Boletín 2024-890.

- El fallo detectado se ocasionaría debido a que el software permitiría ejecutar una firma no válida cuando se utiliza en "modo de reparación". Esto puede generar que un atacante remoto puede engañar a la víctima para que recupere un archivo especialmente diseñado y esto podría comprometer el sistema afectado. Para más información leer el Boletín 2024-891.

- Recientemente, Ivanti advirtió sobre la explotación activa de una vulnerabilidad en su Cloud Services Appliance (CSA), la cual permite a atacantes remotos acceder a funcionalidades restringidas sin autenticación. Para más información leer el Boletín 2024-892.

- Recientemente el equipo de Acronis revelo una falla de seguridad critica en sus complementos de de Acronis Backup, la cual es usada para plataformas de gestión de servidores como cPanel, Plesk y DirectAdmin. Para más información leer el Boletín 2024-894.

- Recientemente el equipo de Microsoft anunció una falla de seguridad de ejecución remota de código, que estaría afectando a la versión de Microsoft Edge basada en Chromium. Para más información leer el Boletín 2024-895.

- La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) ha emitido avisos sobre vulnerabilidades críticas en varios sistemas de control industrial, incluidos el software de Rockwell Automation, PLCs de IDEC y aplicaciones de MegaSys. Estas vulnerabilidades, caracterizadas por altos puntajes de CVSS, presentan riesgos significativos, como la ejecución remota de código y el acceso no autorizado a información sensible. Para más información leer el Boletín 2024-897.

- Recientemente The Browser Company comunico una falla de seguridad critica en el navegador Arc, la cual habría permitido a ciberdelincuentes poder insertar código arbitrario en las sesiones del navegador de otros usuarios. Para más información leer el Boletín 2024-898.

- Según informes de CISA, Versa Networks revelo una vulnerabilidad mediante la cual, ciberdelincuentes podrían aprovechar dicha falla para utilizar API REST no autorizadas. Para más información leer el Boletín 2024-899.

- Recientemente, Camaleon CMS, ha publicado una actualización de seguridad crítica para abordar varias vulnerabilidades, algunas de las cuales ya están siendo explotadas por ciberdelincuentes. Para más información leer el Boletín 2024-900.

- Se ha descubierto una vulnerabilidad crítica en los chipsets wifi de MediaTek, utilizados habitualmente en plataformas integradas que soportan wifi 6 (802.11ax), que permite a los atacantes lanzar ataques de ejecución remota de código (RCE) sin ninguna interacción del usuario. Para más información leer el Boletín 2024-902.

- Recientemente investigadores de seguridad revelaron una falla de seguridad critica en el SDK del complemento de Grafana, que podría provocar la fuga involuntaria de información confidencial. Para más información leer el Boletín 2024-904.

- El proveedor del software ha revelado una vulnerabilidad de ejecución remota de código (RCE) que afecta a su hipervisor bhyve. Esta vulnerabilidad, CVE-2024-41721, podría permitir a los atacantes ejecutar código malicioso en el sistema anfitrión. Para más información leer el Boletín 2024-905.

- Recientemente el equipo de Apache Software Foundation, revelo una vulnerabilidad que podría permitir a ciberdelincuentes poder ejecutar un ataque de denegación de servicio (DoS), afectando a varias versiones de todas sus plataformas. Para más información leer el Boletín 2024-909.

- Recientemente se han descubierto dos vulnerabilidades en el tema de WordPress Houzez, y su complemento Houzez Login Register. Las vulnerabilidades podrían permitir que usuarios no autorizados se apropien de los sitios de WordPress que ejecutan el tema. Para más información leer el Boletín 2024-910.

- Recientemente, se descubre una falla de seguridad, CVE-2024-8956, plantea un riesgo significativo para los usuarios de ciertas cámaras PTZ. Para más información leer el Boletín 2024-911.

- Una vulnerabilidad en los dispositivos de puerta de enlace RAISECOM (MSG1200, MSG2100E, MSG2200, MSG2300) permite la ejecución remota de código no autenticado a través del endpoint vpn/list_base_config.php, debido a una sanitización inadecuada de la entrada en el parámetro template, clasificada como CVE-2024-7120. La explotación implica el envío de solicitudes HTTP manipuladas, con más de 25,000 dispositivos expuestos a internet. Para más información leer el Boletín 2024-914.

- Recientemente el equipo de pgAdmin reveló una falla de seguridad que permitiría a ciberdelincuentes poder comprometer datos de usuarios por medio del mecanismo de autenticación OAuth2. Para más información leer el Boletín 2024-915.

- Recientemente se ha identificado una vulnerabilidad BOLA (CVE-2024-22278) en las versiones de Harbor que permite a los usuarios con un rol de Mantenedor modificar de

manera no autorizada los metadatos del proyecto a través de puntos finales de API. Este exploit elude el control de acceso basado en roles (RBAC), permitiendo acciones maliciosas como hacer que los proyectos sean públicos y eludir los protocolos de escaneo de vulnerabilidades. Para más información leer el Boletín 2024-917.

- Recientemente, los investigadores de seguridad han revelado dos vulnerabilidades en los enrutadores Proroute H685t-w 4G que podrían permitir a ciberdelincuentes remotos comprometer los dispositivos afectados. Para más información leer el Boletín 2024-918.

- Recientemente, TeamViewer ha destacado dos vulnerabilidades que afectan a sus productos Remote Client y Remote Host para Windows. Para más información leer el Boletín 2024-919.

- Recientemente investigadores de seguridad revelaron una vulnerabilidad crítica de inyección SQL en el complemento de WordPress llamado The Events Calendar. Para más información leer el Boletín 2024-920.

- NVIDIA ha informado sobre vulnerabilidades críticas en su Container Toolkit, que podrían permitir a los atacantes ejecutar código remoto. Las vulnerabilidades, identificadas como CVE-2024-0132 y CVE-2024-0133, afectan a todas las versiones de NVIDIA Container Toolkit hasta la versión 1.16.1. Para más información leer el Boletín 2024-921.

- El proveedor Hewlett Packard Enterprise (HPE) ha emitido un aviso crítico relativo a múltiples vulnerabilidades (CVE-2024-42505, CVE-2024-42506, CVE-2024-42507) que afectan a los puntos de acceso Aruba que ejecutan Instant AOS-8 y AOS-10. Estas vulnerabilidades, exponen a los dispositivos afectados a ataques de ejecución remota de código (RCE). Para más información leer el Boletín 2024-922.

- Se han descubierto múltiples vulnerabilidades en el sistema de impresión CUPS que podrían permitir la ejecución remota de código, aunque no afectan a las configuraciones predeterminadas. La explotación requiere que el servicio cups-browsed esté habilitado, lo cual no es común. Para más información leer el Boletín 2024-924.

- Recientemente investigadores de seguridad revelaron una vulnerabilidad de alto riesgo en el Reproductor Multimedia VLC, que permitiría a ciberdelincuentes poder bloquear el programa o incluso ejecutar código arbitrario. Para más información leer el Boletín 2024-925.

- Recientemente el equipo de Progress Software, revelo seis vulnerabilidades críticas en WhatsUp Gold, mediante la cual ciberdelincuentes podrían tener acceso y el control no autorizado de la infraestructura de la red. Para más información leer el Boletín 2024-926.

- Recientemente HashiCorp, ha emitido un aviso de seguridad crítico sobre una vulnerabilidad en su popular herramienta de gestión de secretos. Para más información leer el Boletín 2024-928.

- Recientemente, expertos en ciberseguridad han revelado dos vulnerabilidades críticas en WatchGuard. Para más información leer el Boletín 2024-929.

- Investigadores llegaron a descubrir vulnerabilidades críticas en el complemento Jupiter X Core de WordPress, con la cual, ciberdelincuentes no autenticados podrían tener el control total de un sitio web o secuestrar cuentas de usuario, incluyendo las cuentas con privilegio. Para más información leer el Boletín 2024-930.

- Un equipo de investigación de vulnerabilidades ha revelado dos importantes vulnerabilidades en productos de Microsoft que han sido parcheadas por el proveedor. Para más información leer el Boletín 2024-933.

- Investigadores de seguridad abordaron una vulnerabilidad critica en el kernel de Linux, tras pruebas de conceptos de explotación (POC). Para más información leer el Boletín 2024-934.

- El proveedor de PHP ha publicado recientemente un aviso de seguridad en el que se abordan varias vulnerabilidades que afectan a varias versiones del software. Estas vulnerabilidades van desde la posible manipulación de registros hasta la inclusión de archivos arbitrarios y violaciones de la integridad de los datos. Para más información leer el Boletín 2024-935.

Tendencias en actividades maliciosas

- Medusa, un grupo de ransomware relativamente nuevo, ha adquirido notoriedad por su doble presencia en Internet. A diferencia de sus homólogos, Medusa mantiene un perfil visible en la web junto con sus operaciones en paralelo dentro de la Deep y dark web. Para más información leer el Boletín 2024-877.

- Recientemente, un afiliado del Ransomware Mallox fue detectado utilizando una variante modificada del Ransomware Kryptina para atacar sistemas Linux. Para más información leer el Boletín 2024-912.

- Recientemente, el grupo de ciberamenazas Storm-0501 ha adaptado sus tácticas para atacar entornos de nube híbridos, comprometiendo activos mediante vulnerabilidades y credenciales robadas. Para más información leer el Boletín 2024-927.

4. Detalles

Vulnerabilidades

Boletín	2024-876
Asunto	VULNERABILIDAD EN SPRING FRAMEWORK PERMITIRÍA A LOS ATACANTES OBTENER ACCESO NO AUTORIZADO
Emisión	16/09/2024
CVE	CVE-2024-38816
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Spring Framework 5.3.0 - 5.3.39

• Spring Framework 6.0.0 - 6.0.23

• Spring Framework 6.1.0 - 6.1.12

Descripción

Esta vulnerabilidad, rastreada como CVE-2024-38816, afecta a las aplicaciones que utilizan los frameworks web funcionales WebMvc[.]fn o WebFlux[.]fn. Está clasificada como una vulnerabilidad de path traversal y supone un riesgo para los sistemas afectados.

La vulnerabilidad, CVE-2024-38816, se ocasionaría cuando las aplicaciones sirven recursos estáticos utilizando RouterFunctions combinadas con una ubicación FileSystemResource. Esta configuración puede ser explotada por atacantes que elaboran peticiones HTTP maliciosas para obtener acceso no autorizado a los archivos del sistema.

La vulnerabilidad puede exponer datos sensibles y comprometer la integridad del sistema. Sin embargo, no todos los sistemas que utilizan Spring Framework son vulnerables. Las aplicaciones que emplean el Spring Security HTTP Firewall o se ejecutan en servidores Tomcat o Jetty están protegidas contra estas peticiones maliciosas. Estas configuraciones bloquean y rechazan eficazmente los intentos de explotar la vulnerabilidad.

Para solucionar esta vulnerabilidad crítica, los usuarios de las versiones afectadas deben actualizar a la versión más reciente.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-878
Asunto	ACTUALIZACIÓN DE SEGURIDAD EN ENRUTADORES D-LINK
Emisión	16/09/2024
CVE	Múltiples CVE
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Modelo COVR-X1870 v1.02 y anteriores (Fuera de EE. UU.)

• Modelo DIR-X4860 v1.04B04_Hot-Fix y anteriores (Mundial)

• Modelo DIR-X5460 v1.11B01_Hot-Fix y anteriores (Mundial)

Descripción

Investigadores de seguridad descubrieron vulnerabilidades en enrutadores D-Link, tres de las cuales se consideran críticas. A continuación, se detallan las cinco vulnerabilidades:

CVE-2024-45694 (9.8 crítico): Desbordamiento de búfer basado en pila, que permite a atacantes remotos no autenticados ejecutar código arbitrario en el dispositivo.

CVE-2024-45695 (9.8 crítico): Otro desbordamiento de búfer basado en pila que permite a atacantes remotos no autenticados ejecutar código arbitrario.

CVE-2024-45696 (8.8 alta): Los atacantes pueden habilitar a la fuerza el servicio telnet utilizando credenciales codificadas dentro de la red local.

CVE-2024-45697 (9.8 crítico): el servicio Telnet está habilitado cuando el puerto WAN está conectado, lo que permite el acceso remoto con credenciales codificadas.

CVE-2024-45698 (8.8 alto): La validación de entrada incorrecta en el servicio telnet permite a atacantes remotos iniciar sesión y ejecutar comandos del sistema operativo con credenciales codificadas.

D-Link no ha informado de ninguna explotación de las vulnerabilidades.

Actualización o Mitigación

• Actualizar a v1.03B01 para el modelo COVR-X1870.

• Actualizar a v1.04B05 para el modelo DIR-X4860.

• Actualizar a DIR-X5460A1_V1.11B04 para el modelo DIR-X5460.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Boletín	2024-880
Asunto	VARIOS PROYECTOS EN RIESGO CRITICO DE AUTOGPT
Emisión	17/09/2024
CVE	CVE-2024-6091
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• AutoGPT 0.5.1

Descripción

La vulnerabilidad, descubierta por un investigador de seguridad, implicaba la posible omisión de la lista de denegación de comandos del shell de AutoGPT. Si bien la lista de denegación tenía como objetivo evitar la ejecución de comandos específicos, los ciberdelincuentes podrían eludir fácilmente esta protección utilizando la ruta completa de un comando. Esta falla abrió la puerta a una posible explotación, permitiendo que los ciberdelincuentes ejecutaran acciones no autorizadas en sistemas que ejecutaban AutoGPT.

La capacidad de eludir la lista de comandos rechazados expone los sistemas al riesgo de ejecución de comandos no autorizados. Un ciberdelincuente que aproveche esta vulnerabilidad podría obtener acceso a la información del sistema, aumentar los privilegios y potencialmente, ejecutar comandos arbitrarios, según el contexto en el que se utilice AutoGPT.

Actualización o Mitigación

• Actualizar a la última versión de AutoGPT.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-882
Asunto	MÁS DE 1000 INSTANCIAS DE SERVICENOW FILTRAN DATOS SENSIBLES
Emisión	17/09/2024
CVE	No
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• ServiceNow

Descripción

Se descubrieron más de 1,000 instancias empresariales de ServiceNow mal configuradas que exponían artículos de la base de conocimientos (KB) con información sensible de empresas a usuarios externos y posibles actores de amenazas. Esta información expuesta incluía datos personales (PII), detalles internos de sistemas, credenciales de usuarios, tokens de acceso a sistemas de producción en vivo, entre otros datos críticos, dependiendo del tema de la base de conocimientos.

Aaron Costello, jefe de investigación de seguridad SaaS en AppOmni, identificó que estas instancias de ServiceNow estaban exponiendo información debido a problemas de configuración. A pesar de las actualizaciones que ServiceNow implementó en 2023 para mejorar las listas de control de acceso (ACLs), estas mejoras no se aplicaron a las bases de conocimientos. La plataforma de ServiceNow es una solución en la nube que permite a las organizaciones gestionar flujos de trabajo digitales en distintos departamentos, incorporando gestión de TI, operaciones, tareas de recursos humanos, atención al cliente, integración de herramientas de seguridad, y una base de conocimientos.

El problema radica en que muchas de estas bases de conocimientos, que actúan como repositorios de artículos, contienen información que no debería ser accesible públicamente, como guías internas, procedimientos y datos confidenciales. Aunque ServiceNow lanzó una actualización de seguridad en 2023 que introdujo nuevas ACLs para evitar el acceso no autenticado a datos de clientes, muchos de estos artículos KB siguen utilizando el sistema de permisos "User Criteria" en lugar de las ACLs, lo que hace que la actualización sea menos efectiva. Además, algunos widgets públicos de ServiceNow que exponen información de clientes no recibieron esta actualización, permitiendo así el acceso no autenticado a dichos artículos.

Los controles de acceso mal configurados en estos widgets permiten que actores maliciosos puedan consultar datos en las bases de conocimientos sin necesidad de autenticarse. Los atacantes podrían usar herramientas como Burp Suite para enviar múltiples solicitudes HTTP a un endpoint vulnerable y forzar la enumeración de los números de artículo en la base de conocimientos, ya que estos siguen un formato incremental como KBXXXXXXX.

AppOmni desarrolló un ataque de prueba de concepto para demostrar cómo un actor externo podría acceder a una instancia de ServiceNow, capturar un token para usar en solicitudes HTTP y forzar los números de artículo para encontrar aquellos expuestos de forma involuntaria.

Se sugieren varias propiedades de seguridad que pueden ayudar a proteger los datos incluso en caso de una mala configuración. Entre ellas se encuentran:

• glide.knowman.block_access_with_no_user_criteria (True): Garantiza que el acceso se niegue automáticamente si no se han establecido criterios de usuario.

• glide.knowman.apply_article_read_criteria (True): Exige que los usuarios tengan acceso explícito para leer los artículos.

• glide.knowman.show_unpublished (False): Evita que los usuarios vean artículos en borrador o no publicados.

• glide.knowman.section.view_roles.draft (Admin): Define una lista de roles que pueden ver artículos en estado de borrador.

• glide.knowman.section.view_roles.review (Admin): Define una lista de roles que pueden ver artículos en estado de revisión.

• glide.knowman.section.view_roles.stagesAndRoles (Admin): Define roles que pueden ver artículos en un estado personalizado.

Actualización o Mitigación

• Proteger los artículos de la base de conocimientos configurando correctamente el criterio de usuario ('User Criteria') para bloquear a los usuarios no autorizados. En particular, se deben evitar configuraciones como "Any User" o "Guest User", ya que permiten el acceso arbitrario.

• Si no es indispensable que las bases de conocimientos sean accesibles públicamente, desactivar esta opción para prevenir que artículos internos sean visibles desde internet.

• Se sugiere aplicar las propiedades de seguridad descritas en el boletín para que puedan ayudar a proteger los datos incluso en caso de una mala configuración.

• Se recomienda activar las reglas preconfiguradas de ServiceNow que añaden automáticamente a los usuarios invitados (Guest Users) a la lista de "No puede leer", obligando a los administradores a darles acceso de manera explícita cuando sea necesario.

Boletín	2024-883
Asunto	SOLARWINDS CORRIGE VULNERABILIDADES EN ACCESS RIGHTS MANAGER
Emisión	17/09/2024
CVE	CVE-2024-28991, CVE-2024-28990
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• SolarWinds ARM 2024.3 y versiones anteriores

Descripción

SolarWinds ha lanzado parches para corregir dos vulnerabilidades de seguridad en su software Access Rights Manager (ARM), incluyendo una vulnerabilidad crítica que podría permitir la ejecución remota de código. Esta vulnerabilidad, identificada como CVE-2024-28991, tiene una calificación de 9.0 sobre 10 en el sistema de puntuación CVSS. Se trata de un caso de deserialización de datos no confiables que puede ser explotado para ejecutar código de manera remota.

Según un investigador de seguridad, la falla se encuentra en una clase llamada JsonSerializationBinder y resulta de la falta de validación adecuada de los datos suministrados por el usuario. Esto expone a los dispositivos ARM a una vulnerabilidad de deserialización que podría ser utilizada para ejecutar código arbitrario. Destacando que, aunque se requiere autenticación para explotar la falla, el mecanismo de autenticación existente puede ser eludido.

Además, SolarWinds ha abordado una vulnerabilidad de severidad media en ARM (CVE-2024-28990, CVSS 6.3), que expone una credencial codificada que podría permitir el acceso no autorizado a la consola de administración de RabbitMQ.

Ambos problemas han sido corregidos en la versión 2024.3.1 de ARM. Aunque actualmente no hay evidencia de explotación activa de estas vulnerabilidades.

Actualización o Mitigación

• Actualizar a la versión 2024.3.1 de ARM SolarWinds.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-884
Asunto	VMWARE CORRIGE VULNERABILIDAD CRÍTICA EN VCENTER SERVER
Emisión	17/09/2024
CVE	CVE-2024-38812, CVE-2024-38813
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• VMware vCenter Server

Descripción

Se ha corregido una vulnerabilidad crítica en VMware vCenter Server, identificada como CVE-2024-38812, que permite la ejecución remota de código a través de un paquete de red especialmente diseñado. Esta falla es causada por un desbordamiento de heap en la implementación del protocolo DCE/RPC de vCenter. Además de vCenter, la vulnerabilidad también afecta a productos que lo integran, como VMware vSphere y VMware Cloud Foundation.

Los atacantes no autenticados pueden explotar esta vulnerabilidad de manera remota mediante ataques de baja complejidad que no requieren interacción del usuario, enviando paquetes de red manipulados. También han abordado una vulnerabilidad de escalación de privilegios de alta severidad (CVE-2024-38813), que podría permitir a los atacantes obtener privilegios de root en servidores vulnerables mediante paquetes de red manipulados.

Para mitigar el riesgo, VMware ha publicado parches de seguridad a través de los mecanismos de actualización estándar de vCenter Server.

Aplicar las siguientes actualizaciones:

vCenter Server versión 8.0 -> 8.0 U3b

vCenter Server versión 7.0 -> 7.0 U3s

VMware Cloud Foundation 5.x -> Async patch to 8.0 U3b

VMware Cloud Foundation 4.x -> Async patch to 7.0 U3s

Anteriormente, en enero, se reveló que un grupo de atacantes explotaba una vulnerabilidad crítica en vCenter Server (CVE-2023-34048) como un día cero desde finales de 2021, utilizando este fallo para desplegar puertas traseras en hosts ESXi a través de paquetes de instalación maliciosos.

Actualización o Mitigación

• Aplicar las actualizaciones recomendadas.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-885
Asunto	CISA ADVIERTE SOBRE VULNERABILIDADES EXPLOTADAS EN ADOBE FLASH
Emisión	18/09/2024
CVE	Múltiples CVEs
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Adobe Flash Player anterior a 11.7.700.261 y 11.8.x hasta 12.0.x

• Adobe Flash Player anterior a 10.3.183.67 y 11.x

Descripción

CVE-2013-0643 y CVE-2013-0648: estas fallas críticas de ejecución de código se aprovecharon anteriormente en ataques dirigidos contra usuarios de Firefox.

CVE-2014-0497 y CVE-2014-0502: estas graves vulnerabilidades de desbordamiento de enteros y doble liberación también se explotaron en ataques de día cero.

La explotación continua de estas vulnerabilidades, incluso años después de la desaparición de Flash, pone de relieve el peligro del software obsoleto. Los ciberdelincuentes suelen vulnerar sistemas antiguos, sabiendo que pueden albergar vulnerabilidades sin parches que faciliten el acceso a las redes.

Actualización o Mitigación

• Eliminar el uso de Adobe Flash Player de sus redes, porque ya no ofrece soporte, tampoco actualizaciones de seguridad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-886
Asunto	NUEVAS VULNERABILIDADES EN RED HAT OPENSHIFT
Emisión	18/09/2024
CVE	CVE-2024-45496, CVE-2024-7387
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Red Hat OpenShift Container Platform 4 anterior a la version 0.0.0-alfa.0.0.20240911

• Red Hat OpenShift Container Platform 4 version 4.0.0

Descripción

La primera vulnerabilidad, con una puntuación CVSS de 9,9, **CVE-2024-45496**, es un fallo grave en el proceso de compilación de OpenShift. La vulnerabilidad surge debido a un uso indebido de privilegios elevados durante la inicialización de la compilación, donde el contenedor git-clone se ejecuta con un contexto de seguridad privilegiado. Esto permite a los ciberdelincuentes con acceso a nivel de desarrollador inyectar código malicioso a través de un .gitconfigarchivo creado, lo que da como resultado la ejecución de comandos arbitrarios en el nodo de trabajo.

La segunda vulnerabilidad, **CVE-2024-7387**, con una puntuación CVSS de 9,1, introduce otro riesgo grave para los entornos OpenShift. Esta falla permite la inyección de comandos a través de la ruta de acceso, explotando el spec.source.secrets.secret.destinationDiratributo en la definición de BuildConfig.

Actualización o Mitigación

• Actualizar Red Hat OpenShift Container Platform 4 a la version 0.0.0-alfa.0.0.20240911 o posterior

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-888
Asunto	GITLAB LANZA ACTUALIZACIONES CRÍTICAS PARA CORREGIR VULNERABILIDAD DE ELUSIÓN DE AUTENTICACIÓN SAML
Emisión	18/09/2024
CVE	CVE-2024-45409
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• GitLab 17.3.3, 17.2.7, 17.1.8, 17.0.8, 16.11.10 y todas las versiones anteriores de esas ramas.

Descripción

GitLab ha lanzado actualizaciones de seguridad para abordar una vulnerabilidad crítica de elusión de autenticación SAML que afecta a las instalaciones autogestionadas de las ediciones Community (CE) y Enterprise (EE). Esta vulnerabilidad, identificada como CVE-2024-45409, se origina en problemas dentro de las bibliotecas OmniAuth-SAML y Ruby-SAML, que GitLab utiliza para gestionar la autenticación basada en SAML, un protocolo de inicio de sesión único (SSO) que permite a los usuarios acceder a diferentes servicios con las mismas credenciales.

La vulnerabilidad ocurre cuando la respuesta SAML enviada por un proveedor de identidad (IdP) a GitLab contiene una mala configuración o es manipulada. La falla se debe a una validación insuficiente de elementos clave en las afirmaciones SAML, como el extern_uid (ID de usuario externo), que se utiliza para identificar de manera única a un usuario en diferentes sistemas. Un atacante puede crear una respuesta SAML maliciosa que engañe a GitLab, permitiéndole eludir la autenticación SAML y acceder a la instancia de GitLab como si fuera un usuario autenticado.

Además, GitLab ha proporcionado indicios de posible explotación, como errores de validación de RubySaml, valores inusuales de extern_uid y accesos desde direcciones IP sospechosas.

Actualización o Mitigación

• GitLab ha abordado la vulnerabilidad en las versiones 17.3.3, 17.2.7, 17.1.8, 17.0.8 y 16.11.10, actualizando OmniAuth SAML a la versión 2.2.1 y Ruby-SAML a la 1.17.0. Para aquellos que no puedan actualizar de inmediato, se sugiere habilitar la autenticación de dos factores (2FA).

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-889
Asunto	NUEVA FALLA DE SEGURIDAD EN NEXT JS
Emisión	19/09/2024
CVE	CVE-2024-46982
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Agregar

Descripción

Next.js viene a ser un marco de código abierto que permite a los desarrolladores poder crear aplicaciones web de pila completa con React, pero recientemente investigadores llegaron a detectar fallas que lo hacen vulnerable, específicamente en las versiones entre 13.5.1 y 14.2.9.

La vulnerabilidad identificada fue catalogada como **CVE-2024-46982**, con una puntuación de CVSS de 7.5, la cual es una falla de envenenamiento de caché que amenaza algunas implementaciones de Next.js, especialmente en aquellas que utilizan rutas no dinámicas renderizadas del lado del servidor (SSR) dentro del enrutador de páginas, puesto que al enviar una solicitud HTTP que diseñada a un servidor vulnerable, esta engaña a la aplicación para que almacene en caché las respuestas que no deberían almacenarse.

Los investigadores mencionan que dicha falla de seguridad podría propagarse a las redes de distribución de contenido (CDN) ascendentes, generando consecuencias de alto riesgo, sirviendo contenido envenenado a los usuarios.

Por parte del proveedor, ya ha solucionado los inconvenientes en sus últimas versiones e instan a los usuarios actualizar a la versión parcheada, haciendo mención que no existen soluciones alternativas.

Actualización o Mitigación

• Actualizar Next.js a las versiones 13.5.7, 14.2.12 o posteriores.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática

Boletín	2024-890
Asunto	GOOGLE LANZA UNA NUEVA ACTUALIZACIÓN VARIAS PARA MITIGAR VARIAS VULNERABILIDADES
Emisión	19/09/2024
CVE	CVE-2024-8904, CVE-2024-8905, CVE-2024-8906, CVE-2024-8907, CVE-2024-8908, CVE-2024-8909
Categoría	Actualización
Severidad	ALTA

Servicios Afectados

• Anteriores a Google Chrome 129.0.6668.58 para Linux

• Anteriores a Google Chrome 129.0.6668.58/.59 para Windows y Mac

Descripción

Los detalles de estas correcciones permanecerán restringidos hasta que la mayoría de los usuarios hayan actualizado sus navegadores para garantizar la seguridad en todas las plataformas.

El CVE-2024-8904 es una vulnerabilidad de confusión de tipo en V8 y tiene severidad alta.

El CVE-2024-8905 es una vulnerabilidad ocasionada por la implementación inadecuada en V8 con una severidad media.

El CVE-2024-8906 es una vulnerabilidad que inducía al usuario para que realizara gestos específicos de la interfaz de usuarioMedia a través de una página HTML diseñada; está catalogado con una severidad media.

El CVE-2024-8907 es un fallo en la validación de datos en Omnibox y tiene una severidad media.

El CVE-2024-8908 es una vulnerabilidad ocasionada por la inadecuada implementación de Autofill y tiene una severidad baja.

El CVE-2024-8909 es una vulnerabilidad en la implementación de UI y tiene una severidad baja.

Además de estos problemas notificados, el equipo de Chrome ha implementado varias correcciones de seguridad internas mediante auditorías, fuzzing y otras iniciativas. El proveedor recomendó a los usuarios que actualicen sus navegadores.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-891
Asunto	NUEVA VULNERABILIDAD EN LIBREOFFICE
Emisión	19/09/2024
CVE	CVE-2024-7788
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• LibreOffice versiones anteriores a 24.2.5 y 24.8.0

Descripción

LibreOffice es una popular suite ofimática de código abierto que soporta varios formatos de archivo que se basan en la estructura de archivos ZIP.

Cuando estos archivos se dañan, el modo de reparación de LibreOffice intenta recuperar el documento reconstruyendo la estructura del archivo ZIP. Sin embargo, se ha identificado una vulnerabilidad en este proceso.

Antes de la reciente corrección, los atacantes habrían explotado este mecanismo de reparación creando un documento que, una vez reparado, informara incorrectamente del estado de la firma digital como “no válida”. Esto podía inducir a los usuarios a confiar en documentos manipulados.

La vulnerabilidad afecta principalmente a los archivos ZIP firmados digitalmente. Un atacante podría crear un documento corrupto que, al abrirse en el modo de reparación de LibreOffice, eludiera la verificación de la firma. Esto significa que los usuarios podrían activar inadvertidamente macros o confiar en contenidos que podrían ser maliciosos.

En versiones anteriores de LibreOffice, los usuarios podían ignorar los fallos de verificación y podían a habilitar las macros. Este comportamiento planteaba importantes riesgos de seguridad, ya que las macros maliciosas podían ejecutar código dañino en el sistema de un usuario.

Las versiones 24.2.5 y 24.8.0 de LibreOffice solucionan la vulnerabilidad. En estas versiones actualizadas, todas las firmas se consideran automáticamente inválidas cuando se abre un documento en modo de reparación. El fallo fue catalogado como CVE-2024-7788.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-892
Asunto	ACTUALIZACIÓN DE SEGURIDAD CORRIGE VULNERABILIDAD EN IVANTI
Emisión	19/09/2024
CVE	CVE-2024-8963
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Ivanti Cloud Services Appliance (CSA) versión 4.6

Descripción

Ivanti advirtió sobre la explotación activa de una nueva vulnerabilidad en su Cloud Services Appliance (CSA), que está afectando a un número limitado de clientes. Esta vulnerabilidad, identificada como CVE-2024-8963, permite la omisión de autenticación de administrador debido a una debilidad de traversal de ruta. Si es explotada con éxito, permite a atacantes remotos no autenticados acceder a funcionalidades restringidas en los sistemas vulnerables de CSA, los cuales son utilizados para proporcionar acceso seguro a los usuarios empresariales a los recursos internos de la red.

Los atacantes están utilizando exploits que combinan CVE-2024-8963 con la vulnerabilidad CVE-2024-8190, un fallo grave de inyección de comandos en CSA que fue corregido recientemente y clasificado como activamente explotado. Esta combinación de vulnerabilidades permite a los atacantes eludir la autenticación de administrador y ejecutar comandos arbitrarios en dispositivos que no han sido parcheados.

Según Ivanti, la vulnerabilidad fue descubierta durante la investigación de los ataques relacionados con la explotación que la empresa divulgó el 13 de septiembre. En el proceso de análisis, identificaron que el problema había sido parcialmente abordado de manera incidental con la eliminación de ciertas funcionalidades en el parche 519.

Ivanti recomienda a los administradores revisar alertas de soluciones de detección y respuesta de endpoints (EDR) u otro software de seguridad, así como la configuración y los privilegios de acceso de usuarios administrativos para detectar posibles intentos de explotación. Además, se sugiere configurar el CSA con eth0 como red interna para reducir significativamente el riesgo de ataques.

En caso de sospecha de compromiso, Ivanti aconseja reconstruir el sistema CSA utilizando el parche 519, lanzado el 10 de septiembre de 2024, y migrar a la versión CSA 5.0, si es posible.

Actualización o Mitigación

• Migrar a la versión CSA 5.0 siempre que sea posible, ya que la versión 4.6 ha alcanzado su fin de vida y no recibirá más actualizaciones de seguridad.

• Revisar alertas de seguridad en soluciones EDR y otros sistemas de detección para identificar intentos de explotación o usuarios administrativos nuevos o modificados.

• Revisar configuraciones y accesos para limitar los privilegios de los usuarios administrativos y detectar cualquier modificación no autorizada.

Boletín	2024-894
Asunto	NUEVA FALLA DE SEGURIDAD CRITICA EN ACRONIS
Emisión	19/09/2024
CVE	CVE-2024-8767
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Complemento Acronis Backup para cPanel y WHM (Linux) anterior a la compilación 619

• Extensión Acronis Backup para Plesk (Linux) anterior a la compilación 555.

• Complemento Acronis Backup para DirectAdmin (Linux) anterior a la compilación 147.

Descripción

Según investigadores, la vulnerabilidad critica estaría afectando al complemento Acronis Backup y directamente para Linux en platafromas como cPanel & WHM, Plesk y DirectAdmin, ya que este es usado para automatizar las copias de seguridad de servidores y sitios web.

La falla reside en la configuración de permisos que lleva dentro de los complementos, provocando la filtración de información confidencial además de permitir operaciones no autorizadas en los servidores afectados.

La vulnerabilidad identificada fue catalogada como **CVE-2024-8767**, con una puntuación de CVSS de 9.9, la cual hace referencia a la divulgación y manipulación de datos confidenciales debido a la asignación innecesaria de privilegios. Los investigadores mencionan que, de no llevar a cabo las actualizaciones pertinentes, los servidores que ejecutan tales complementos afectados podrían correr el riesgo de sufrir graves violaciones o manipulaciones de datos.

Por parte del proveedor, ya ha solucionado los inconvenientes publicando parches de actualización para dicha falla, haciendo mención que no existen soluciones alternativas.

Actualización o Mitigación

• Actualizar complementos con nuevos parches publicados por el equipo de Acronis.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-895
Asunto	NUEVA FALLA DE SEGURIDAD DE RCE EN MICROSOFT EDGE
Emisión	20/09/2024
CVE	CVE-2024-43496
Categoría	Vulnerabilidad
Severidad	MEDIA

Servicios Afectados

• Microsoft Edge

Descripción

Recientemente Microsoft reveló una grave vulnerabilidad de ejecución remota de código (RCE) que afecta a la versión basada en Chromium de Microsoft Edge, la vulnerabilidad fue identificada como **CVE-2024-43496**, con una puntuación de CVSS de 6.5.

Es importante mencionar que una vulnerabilidad de ejecución remota de código es de riesgo significativo, ya que pueden permitir a ciberdelincuentes poder ejecutar código arbitrario en el sistema afectado, ocasionando graves infracciones de seguridad, asimismo podrían explotar fallas en el software para ejecutar código malicioso sin el consentimiento del usuario, es por ello que los atacantes pueden aprovechar este tipo de falla a través de páginas web maliciosas, correos electrónicos maliciosos o incluso a través de sitios web comprometidos.

SI hablamos de impacto, los investigadores mencionan que un tipo de vulnerabilidad como este podría permitir la manipulación de datos de usuarios y acceder a información confidencial, instalación de malware adicional en sistemas comprometidos o poder realizar más ataques a redes y dispositivos conectados por parte de atacantes.

Por parte de Microsoft y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), aún se encuentran trabajando en dicha vulnerabilidad, por lo que se espera las recomendaciones pertinentes.

Actualización o Mitigación

• Monitorear al lanzamiento de parches y actualizaciones por parte de Microsoft.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Boletín	2024-897
Asunto	CISA ADVIERTE SOBRE VULNERABILIDADES CRÍTICAS EN SISTEMAS DE CONTROL INDUSTRIAL
Emisión	20/09/2024
CVE	Múltiples CVEs
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• RSLogix 500, RSLogix Micro Developer y Starter, RSLogix 5 y las versiones anteriores.

• Módulos CPU, MICROSmart Series FC6A y FC6B (versiones 2.60 y anteriores) y el SmartAXIS Pro/Lite Serie FT1A (versiones 2.41 y anteriores).

• WindLDR versión 9.1.0 y anteriores y WindO/I-NV4 versión 3.0.1 y anteriores.

• La aplicación web Telenium Online 8.3 y las versiones anteriores; Las versiones de firmware anteriores al 1 de mayo de 2024 se ven afectadas; La pila de TCP/IP de Treck anterior a 6.0.1.66.

Descripción

CISA ha publicado seis avisos sobre vulnerabilidades críticas de varios sistemas de control industrial.

Una vulnerabilidad notable se encuentra en el software RSLogix 5 y RSLogix 500 de Rockwell Automation, identificado como CVE-2024-7847, que tiene un puntaje CVSS v4 de 8.8. El defecto surge de una verificación insuficiente de la autenticidad de los datos, lo que permite a los atacantes incrustar scripts VBA maliciosos en los archivos de proyecto. Esta vulnerabilidad puede facilitar la ejecución remota de código sin intervención del usuario.

Los PLC de IDEC Corporation también presentan vulnerabilidades críticas, notablemente la transmisión en texto claro de información sensible y la generación de identificadores predecibles. Identificadas como CVE-2024-41927 y CVE-2024-28957, estas vulnerabilidades, con un puntaje CVSS v3 de 5.3, podrían llevar a un acceso no autorizado a los datos de autenticación de los usuarios.

El software WindLDR y WindO/I-NV4 de IDEC Corporation está comprometido debido al almacenamiento en texto claro de información sensible (CVE-2024-41716), con un puntaje de 5.9. La explotación exitosa de esta vulnerabilidad podría resultar en el acceso no autorizado a las credenciales de usuario. De manera similar, la aplicación web Telenium de MegaSys Computer Technologies enfrenta una vulnerabilidad severa (CVE-2024-6404) debido a la validación incorrecta de entrada, que permite a los atacantes inyectar código Perl arbitrario de forma remota.

Además, Kastle Systems está en riesgo debido a credenciales codificadas de forma fija (CVE-2024-45861) y vulnerabilidades de almacenamiento en texto claro (CVE-2024-45862), ambas con un puntaje CVSS v4 de 9.2. El stack TCP/IP de Treck también ha sido identificado con múltiples vulnerabilidades críticas, incluidas el manejo incorrecto de parámetros de longitud, que podrían permitir la ejecución remota de código.

Actualización o Mitigación

• Se recomienda a las organizaciones que utilizan estos sistemas a implementar actualizaciones a tiempo.

Boletín	2024-898
Asunto	FALLA DE SEGURIDAD CRITICA EN ARC HABRIA PERMITIDO ACCESO EN NAVEGADORES
Emisión	20/09/2024
CVE	CVE-2024-45489
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Navegador web ARC.

• Sistemas operativos Windows y macOS.

Descripción

Según investigadores de seguridad la falla de seguridad habría permitido a los atacantes poder insertar código arbitrario en las sesiones de navegadores de otros usuarios con solo el ID de usuario.

La vulnerabilidad identificada fue catalogada como **CVE-2024-45489**, con una puntuación de CVSS de 9.8, mediante la cual se permite la ejecución remota de código en boosts de JavaScript, según el equipo de The Browser Company, la falla de seguridad fue parcheada el 26 de agosto, pero que se divulgo recientemente, haciendo mención que sus registros indican que ningún usuario se vio afectado por la falla.

La **CVE-2024-45489**, reside en la configuración incorrecta en la implementación de Firebase de The Browser Company, conocido como un servicio de base de datos como backend, esto para el almacenamiento de información del usuario, incluidos Arc Boosts, la cual permite a usuarios poder personalizar la apariencia de los sitios web que visitan.

Por parte del proveedor continúan trabajando en mejoras para actualizaciones en Arc.

Actualización o Mitigación

• Aplicar los parches más recientes para protegerse contra posibles amenazas.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Boletín	2024-899
Asunto	NUEVA FALLA DE SEGURIDAD EN VERSA DIRECTOR
Emisión	21/09/2024
CVE	CVE-2024-45229
Categoría	Vulnerabilidad
Severidad	MEDIA

Servicios Afectados

• Versa Director.

• Sistemas operativos Windows.

Descripción

Versa Director es una plataforma que ofrece API REST para orquestación y administración, en la cual algunas API como como la pantalla de inicio de sesión, la visualización de banners y el registro de dispositivos, no requieren autenticación, es por ello que recientemente el equipo de Versa reveló que una de estas API se puede explotar inyectando argumentos no válidos en una solicitud GET, exponiendo los tokens de autenticación de usuarios que hayan iniciado sesión en ese momento, los cuales pueden invocar API adicionales en el puerto 9183.

Los investigadores mencionan que el exploit no revela ninguna información de nombre de usuario o contraseña, la vulnerabilidad fue identificada como **CVE-2024-45229** con una puntuación de CVSS de 6,6, y que esta falla de seguridad no puede ser explotada en los Directors de Versa que no estén expuestos a Internet.

Por parte del proveedor y de CISA, instan a los usuarios mantenerse con las ultimas actualizaciones.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-900
Asunto	NUEVAS VULNERABILIDADES EN CAMALEON CMS
Emisión	21/09/2024
CVE	CVE-2024-46986, CVE-2024-46987
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Camaleon CMS versión 2.8.0

Descripción

La vulnerabilidad más alarmante, identificada como **CVE-2024-46986**, es una falla de escritura arbitraria de archivos que permite a los usuarios autenticados escribir archivos en cualquier ubicación del servidor. Esto podría permitir a los ciberdelincuentes ejecutar código malicioso de forma remota, lo que podría comprometer todo el sitio web y cualquier dato asociado.

Otra vulnerabilidad crítica, **CVE-2024-46987**, implica un problema de cruce de ruta que permite el acceso no autorizado a archivos confidenciales en el servidor. Esto podría provocar la exposición de información confidencial, lo que pone en mayor riesgo la seguridad del sitio web afectado.

A las preocupaciones se suma una vulnerabilidad de secuencias de comandos entre sitios almacenadas en la función de carga de imágenes. Esta falla permite a los ciberdelincuentes inyectar código JavaScript malicioso en imágenes o documentos cargados, que, cuando son vistos por usuarios desprevenidos, pueden desencadenar varias acciones maliciosas, como robar cookies de sesión o modificar el contenido del sitio web.

Actualización o Mitigación

• Actualizar Camaleon CMS a la versión 2.8.2, para corregir la vulnerbilidad.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-902
Asunto	UNA VULNERABILIDAD EN LOS CHIPSETS WIFI PERMITIRÍA EXPLOTACIÓN REMOTA
Emisión	22/09/2024
CVE	CVE-2024-20017
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Chipsets wifi de MediaTek

Descripción

Esta vulnerabilidad, CVE-2024-20017, afecta a una amplia gama de dispositivos de fabricantes como Ubiquiti, Xiaomi y Netgear.

La vulnerabilidad reside en el daemon de red wappd, que forma parte del SDK MediaTek MT7622/MT7915 y del paquete de controladores RTxxxx SoftAP. Se utiliza principalmente para configurar y coordinar interfaces inalámbricas y puntos de acceso que utilizan Hotspot 2.0 y tecnologías afines.

El fallo es un desbordamiento de búfer causado por una operación de copia que utiliza un valor de longitud tomado directamente de los datos del paquete controlado por el atacante sin comprobación de límites, lo que permite que hasta 1433 bytes de datos controlados por el atacante desborden la pila. Los investigadores han desarrollado cuatro exploits diferentes para este fallo.

El primer exploit demuestra un secuestro del puntero de instrucción de retorno (RIP), utilizando el desbordamiento de pila para corromper la dirección de retorno guardada y redirigir la ejecución a un gadget ROP que llama a system() para ejecutar comandos de shell.

El segundo exploit elude los stack canaries de pila y ASLR corrompiendo un puntero para conseguir escritura arbitraria. Esto se utiliza para sobrescribir la entrada GOT (Global Offset Table) de read() con la dirección de un gadget ROP, que luego salta a system() para ejecutar una payload de shell.

El tercer exploit, dirigido a una versión con RELRO (Read-Only Relocations) completo, utiliza ROP para obtener de manera arbitraria el write primitive. Esta encadena gadgets para escribir un valor arbitrario de 8 bytes en una dirección arbitraria, escribiendo finalmente un comando shell en los segmentos .bss o .data. Este exploit salta entonces a una cadena ROP final que coloca la dirección del comando shell en el registro apropiado y llama al system().

El cuarto exploit está dirigido al Netgear WAX206, que tiene ASLR, NX, RELRO completo y stack canaries habilitados. Debido al inlining de funciones y a la semántica arm64, la estrategia del exploit tuvo que ser adaptada. Utiliza la corrupción de punteros para lograr de forma arbitraria el write primitive a través del puntero pPktBuf y luego corrompe la dirección de retorno guardada en el marco de pila para IAPP_RcvHandler().

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus.

Boletín	2024-904
Asunto	NUEVA FALLA DE SEGURIDAD CRITICA EN GRAFANA
Emisión	23/09/2024
CVE	CVE-2024-8986
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Grafana

Descripción

Según los investigadores, la vulnerabilidad podría ocasionar una fuga involuntaria de información confidencial, incluyendo las credenciales del repositorio.

El SDK del complemento Grafana incluye metadatos de compilación en los binarios que este compila, ya que estos metadatos incluyen la URL del repositorio para el complemento que se está compilando, tal como se obtiene al ejecutar `git remote get-url origin`. Es por ello que, si se incluyen credenciales en la URL del repositorio como, por ejemplo, para permitir la obtención de dependencias privadas), el binario final contendrá el URI completo, incluyendo dichas credenciales.

La vulnerabilidad identificada fue catalogada como **CVE-2024-8986**, con una puntuación de CVSS de 9.1, por lo que mediante dicha falla se podría permitir a ciberdelincuentes, poder obtener acceso a un complemento creado con las versiones afectadas del SDK. logrando extraer fácilmente estas credenciales integradas, otorgándole el acceso no autorizado a repositorios privados y al código o los datos confidenciales que contienen.

Asimismo, investigadores resaltan que la vulnerabilidad no presenta complicaciones para ser explotada, haciendo mención que todas las versiones del SDK del complemento Grafana para Go hasta la versión 0.249.0 estarían siendo afectados.

Actualización o Mitigación

• Actualizar versiones de SDK de Grafana a la versión 0.250.0 o posterior.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-905
Asunto	NUEVA ACTUALIZACIÓN DE SEGURIDAD EN FREEBSD
Emisión	23/09/2024
CVE	CVE-2024-41721
Categoría	Actualización
Severidad	ALTA

Servicios Afectados

• FreeBSD

Descripción

Según un informe, la vulnerabilidad reside en la emulación XHCI del hipervisor bhyve, que se utiliza para ejecutar sistemas operativos invitados dentro de máquinas virtuales. En concreto, el fallo se debe a una validación de límites insuficiente en el código USB, que provoca una lectura fuera de los límites de la pila.

Este fallo puede ser aprovechado por software malicioso que se ejecute en una máquina virtual huésped para bloquear el proceso del hipervisor o lograr la ejecución de código en el sistema anfitrión. El proceso bhyve suele ejecutarse como root, lo que aumenta el impacto potencial de esta vulnerabilidad.

Aunque bhyve funciona dentro de un sandbox, que limita las capacidades disponibles para los procesos, esto no mitiga por completo el riesgo que plantea esta vulnerabilidad. Los sistemas que utilizan emulación XHCI están particularmente en riesgo.

Esta vulnerabilidad afecta a todas las versiones soportadas de FreeBSD. Su impacto potencial es significativo, ya que permite a atacantes con acceso privilegiado a máquinas virtuales huéspedes ejecutar código arbitrario en el sistema anfitrión. Esto podría dar lugar a un acceso o control no autorizado sobre la máquina anfitriona, lo que supone una grave amenaza para la seguridad de los sistemas afectados.

Para mitigar esta vulnerabilidad, los usuarios deben actualizar sus sistemas FreeBSD a una versión que incluya el parche publicado el 19 de septiembre de 2024. Según el proveedor, el proyecto FreeBSD ofrece dos métodos para actualizar los sistemas afectados.

Actualización del parche binario. Los sistemas que ejecutan una versión RELEASE de FreeBSD pueden actualizarse mediante la utilidad FreeBSD-update. Esto implica la obtención e instalación de las últimas actualizaciones mediante instrucciones en la línea de comandos.

Actualización de parches de código fuente: Los usuarios pueden descargar y verificar los parches desde el sitio web de seguridad de FreeBSD y aplicarlos manualmente mediante herramientas de línea de comandos. Este método requiere recompilar el sistema operativo utilizando los procedimientos build world e install world.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2024-909
Asunto	NUEVA FALLA DE SEGURIDAD EN APACHE TOMCAT
Emisión	24/09/2024
CVE	CVE-2024-38286
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Apache Tomcat.

Descripción

La vulnerabilidad identificada fue catalogada como **CVE-2024-38286**, relacionada con el agotamiento de los recursos en Apache Tomcat, la cual podría permitir a un ciberdelincuente de manera remota, poder realizar un ataque de DoS.

Según los investigadores esta falla de seguridad reside debido a que la aplicación no controla adecuadamente el consumo de recursos internos durante el proceso de enlace TLS, por lo que un atacante remoto puede iniciar múltiples conexiones TLS, provocar el agotamiento de la memoria y de esa manera poder realizar un ataque de DoS, también un atacante tendría que enviar una solicitud directamente a la aplicación afectada. Asimismo, los investigadores que un atacante podría explotar esta falla para provocar un OutOfMemoryError, lo que provocaría un bloqueo del servidor y la interrupción de cualquier servicio que dependa de él.

Dentro del impacto de la falla, se menciona que podría ocasionar una Interrupción del servicio, por lo que las aplicaciones y servicios críticos que se ejecutan en Tomcat podrían dejar de estar disponibles, de igual manera podría existir un agotamiento de recursos y tiempo de inactividad operativo.

Las siguientes versiones de Apache Tomcat se ven afectadas serian: 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, por ello, por parte de Apache Software Foundation, solucionaron los inconvenientes en sus últimas versiones.

Actualización o Mitigación

• Mantener actualizado Apache Tomcat, en sus últimas versiones.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-910
Asunto	NUEVAS VULNERABILIDADES EN WORDPRESS HOUZEZ
Emisión	24/09/2024
CVE	CVE-2024-22303, CVE-2024-21743
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Houzez de WordPress versiones 3.2.4 y anteriores

• Houzez de WordPress versiones 3.2.5 y anteriores

Descripción

Los investigadores de seguridad han descubierto una vulnerabilidad (**CVE-2024-22303**) de escalada de privilegios no autenticados en el tema Houzez. Esta falla podría permitir que cualquier usuario no autenticado eleve sus privilegios y potencialmente tome el control de un sitio de WordPress mediante la realización de una serie de solicitudes HTTP.

La vulnerabilidad existe porque el código que maneja la entrada del usuario carece de las comprobaciones de autorización adecuadas. Si bien el tema incluye una comprobación de nonce, cualquier usuario con un rol de suscriptor puede recuperar el nonce. Si el registro de usuarios está habilitado en el sitio, incluso los usuarios no autenticados pueden registrarse y obtener el token de nonce.

Esta vulnerabilidad (**CVE-2024-21743**) podría permitir que un actor malintencionado escale su cuenta con pocos privilegios a una con privilegios más altos. Después de esto, podría tomar el control total del sitio web si obtiene privilegios altos.

Actualización o Mitigación

• Actualizar Houzez de WordPress a las versiones 3.3.0 o posteriores.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-911
Asunto	LAS CAMARAS PTZOPTICS SON VULNERABLES A ATAQUES REMOTOS
Emisión	24/09/2024
CVE	CVE-2024-8956
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• PTZOptics PT30X-SDI (versiones anteriores a 6.3.40)

• PTZOptics PT30X-NDI-xx-G2 (versiones anteriores a 6.3.40)

• Otros equipos AV que utilizan el firmware de cámara PTZ de ValueHD Corporation.

Descripción

La causa principal de **CVE-2024-8956** es un mecanismo de autenticación insuficiente. En concreto, los dispositivos afectados no aplican la autenticación adecuada a las solicitudes enviadas al punto final cuando no se incluye ningún encabezado de autorización HTTP. Esta falla permite que un ciberdelincuente remoto, sin ninguna autenticación, recupere datos confidenciales, incluidos nombres de usuario, hashes de contraseñas y detalles de configuración.

Peor aún, la vulnerabilidad permite a los ciberdelincuentes no solo ver datos confidenciales, sino también alterar valores de configuración o sobrescribir archivos de configuración completos. En términos prácticos, esto podría dar como resultado el secuestro del control de la cámara, la alteración de las configuraciones de seguridad y un uso potencialmente malicioso del dispositivo para futuras vulnerabilidades en la red.

Actualización o Mitigación

• Actualizar firmware de PTZOptics a la versión 6.3.40.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-914
Asunto	VULNERABILIDAD EN DISPOSITIVOS GATEWAY RAISECOM
Emisión	24/09/2024
CVE	CVE-2024-7120
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Modelos de puerta de enlace RAISECOM MSG1200, MSG2100E, MSG2200, MSG2300, para la versión 3.90.

Descripción

A finales de julio, un investigador reveló una vulnerabilidad significativa que afecta a los dispositivos de puerta de enlace RAISECOM. Esta vulnerabilidad, ubicada en el endpoint "vpn/list_base_Config.php", permite la ejecución remota de código no autenticada, exponiendo así un número considerable de dispositivos a posibles explotaciones.

Tras la publicación, comenzaron a surgir intentos de explotación de esta vulnerabilidad, siendo los primeros ataques detectados por los sensores de seguridad el 1 de septiembre. Los ataques observados utilizan principalmente dos cargas útiles distintas, ambas con la capacidad de ejecutar comandos arbitrarios en los dispositivos comprometidos. La primera carga útil emplea una secuencia de comandos para descargar y ejecutar un archivo malicioso a través de HTTP, mientras que la segunda utiliza TFTP para la recuperación de archivos, lo que indica la presencia de un esfuerzo coordinado para explotar estas vulnerabilidades.

Un examen exhaustivo de la vulnerabilidad revela que afecta a modelos específicos de puerta de enlace RAISECOM, incluyendo el MSG1200, MSG2100E, MSG2200 y MSG2300, así como a dispositivos que ejecutan la versión de software 3.90. La raíz del problema radica en el script list_base_config.php, donde el manejo inadecuado del parámetro template facilita los ataques de inyección de comandos. Esta falta de saneamiento de entrada es un descuido crítico que permite a los atacantes manipular el sistema a través de la interfaz web.

Actualización o Mitigación

• Implementar comprobaciones de validación en las entradas que pueden afectar a los comandos del sistema o las rutas de archivos.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-915
Asunto	FALLA CRITICA EN PG ADMIN EXPONE DATOS CONFIDENCIALES
Emisión	25/09/2024
CVE	CVE-2024-9014
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• pgAdmin

Descripción

pgAdmin viene a ser una herramienta líder de gestión de código abierto para bases de datos PostgreSQL, por lo que recientemente su equipo lanzo una actualización para solucionar los inconvenientes de esta nueva falla seguridad crítica que afecta a las versiones 8.11 y anteriores.

La vulnerabilidad identificada fue catalogada como **CVE-2024-9014** y con una puntuación CVSS de 9,9, dicha falla podría permitir que un atacante obtenga potencialmente el ID y el secreto del cliente, lo que lleva a un acceso no autorizado a los datos del usuario, y que asimismo los datos de los usuarios sean comprometidos por los atacantes a través del mecanismo de autenticación OAuth2, como impacto podría provocar violaciones de datos y un mayor compromiso del sistema.

Según investigadores la falla de seguridad se origina en la implementación de autenticación OAuth2 de pgAdmin, por parte del proveedor instan a usuarios llevar a cabo las actualizaciones que estaría garantizando que sus entornos PostgreSQL estén protegidos contra la posible explotación.

Actualización o Mitigación

• Actualizar pgAdmin a la versión 8.12 o posteriores.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-917
Asunto	VULNERABILIDAD BOLA EN HARBOR EXPONE METADATOS DE PROYECTO A TRAVÉS MODIFICACIONES NO AUTORIZADAS
Emisión	25/09/2024
CVE	CVE-2024-22278
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Las versiones de Harbor anteriores a 2.9.5.

Descripción

Investigadores han identificado recientemente una vulnerabilidad crítica de autorización a nivel de objeto rota (BOLA), designada como CVE-2024-22278, en las versiones de Harbor anteriores a la 2.9.5. Harbor es un prominente registro de contenedores nativo de la nube que facilita la gestión y el alojamiento de imágenes de contenedores. Ofrece características vitales, incluyendo control de acceso basado en roles (RBAC), escaneo de vulnerabilidades y firma de imágenes. La vulnerabilidad BOLA permite a los usuarios con el rol de Mantenedor realizar acciones no autorizadas sobre los metadatos del proyecto, específicamente, la capacidad de crear, actualizar y eliminar metadatos, lo que contraviene los permisos explícitamente asignados dentro del sistema. Esta desalineación entre los roles de usuario presenta riesgos significativos, incluyendo la exposición de datos y la elusión de los protocolos establecidos de escaneo de vulnerabilidades.

El descubrimiento de esta vulnerabilidad surgió durante el desarrollo de una herramienta automatizada de detección de BOLA que utiliza inteligencia artificial generativa, como parte de una iniciativa más amplia para mejorar las medidas de seguridad a través de la inteligencia artificial. Notablemente, la investigación destacó inconsistencias entre la interfaz de usuario web de Harbor y la API subyacente. Mientras que la interfaz de usuario restringe a los Mantenedores de modificar los metadatos del proyecto, la API permite tales modificaciones a través de solicitudes válidas. Esta discrepancia socava significativamente la postura de seguridad de Harbor, ya que habilita actividades maliciosas potenciales que podrían comprometer la integridad de los proyectos alojados.

Las consecuencias de tal explotación pueden extenderse más allá de las brechas de datos inmediatas, dañando potencialmente la confianza y el marco de seguridad general de los entornos afectados.

Actualización o Mitigación

• Actualiza Harbor a la versión v2.9.5, v2.10.3 o v2.11.0.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-918
Asunto	NUEVAS VULNERABILIDADES EN EL ENRUTADOR PROROUTE H685T-W 4G
Emisión	26/09/2024
CVE	CVE-2024-45682, CVE-2024-38380
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Proroute H685t-w versión 3.2.334

Descripción

La vulnerabilidad **CVE-2024-45682** podría ser explotada por cualquier usuario con acceso a la interfaz web del enrutador, incluso con privilegios limitados. El ciberdelincuente podría obtener el control total del dispositivo, lo que le permitiría realizar acciones como instalar malware, extraer información confidencial o lanzar más ataques a la red conectada.

La segunda vulnerabilidad, identificada como **CVE-2024-38380**, es un error de tipo cross-site scripting (XSS) que podría permitir a un ciberdelincuente inyectar scripts maliciosos en las páginas web que visitan los usuarios del enrutador afectado. Esta vulnerabilidad podría aprovecharse para robar cookies de sesión, secuestrar cuentas de usuario o lanzar ataques de phishing.

Actualización o Mitigación

• Actualizar 4G H685t-w a las versiones firmware 3.2.335 o posterior.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-919
Asunto	NUEVAS VULNERABILIDADES EN TEAMVIEWER
Emisión	26/09/2024
CVE	CVE-2024-7479, CVE-2024-7481
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• TeamViewer Remote Clients versión anterior a la 15.58.4

• Sistemas operativos Windows

Descripción

La vulnerabilidad **CVE-2024-7479** implica la verificación incorrecta de la firma criptográfica durante la instalación de un controlador VPN.

La vulnerabilidad **CVE-2024-7481** implica la verificación incorrecta de la firma criptográfica durante la instalación de un controlador de impresora.

Estas vulnerabilidades permiten a los ciberdelincuentes con acceso local sin privilegios aumentar sus privilegios e instalar controladores maliciosos en el sistema afectado. Una vez que se instala un controlador malicioso, los ciberdelincuentes pueden ejecutar código con privilegios elevados y obtener así el control total de la máquina.

Para explotar estas vulnerabilidades, los ciberdelincuentes deben tener acceso local al sistema Windows. Si bien la explotación remota no es posible, una vez que un ciberdelincuente tiene acceso local, el potencial de daño es grave. Al aumentar los privilegios, el ciberdelincuente puede eludir los controles de seguridad del sistema, instalar software no autorizado o manipular archivos críticos del sistema.

Actualización o Mitigación

• Actualizar TeamViewer Remote Clients versión 15.58.4 o posteriores.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-920
Asunto	NUEVA FALLA DE SEGURIDAD CRITICA EN WORDPRESS
Emisión	26/09/2024
CVE	CVE-2024-8275
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• WordPress

Descripción

El complemento afectado permite a usuarios poder crear y administrar calendarios de eventos sin esfuerzo en sitios de WordPress, asimismo este admite eventos presenciales y virtuales ofreciendo una variedad de diversas funciones.

La vulnerabilidad identificada fue catalogada como **CVE-2024- 8275**, con una puntuación CVSS de 9,8, haciendo referencia que el complemento es vulnerable a la inyección SQL a través del parámetro 'order' de la función 'tribe_has_next_event' en todas las versiones hasta la 6.6.4 inclusive, debido a un escape insuficiente en el parámetro proporcionado por el usuario y a la falta de preparación suficiente en la consulta SQL existente, haciendo posible que ciberdelincuentes no autentificados puedan agregar consultas SQL adicionales a consultas ya existentes y estas se puedan usar para extraer información confidencial de la base de datos.

Según los investigadores solos los sitios que hayan agregado manualmente la función tribe_has_next_event() son vulnerables a esta inyección SQL, siendo este el origen de dicha falla de segurida.

Actualización o Mitigación

• Actualizar el complemento The Events Calendar a la versión 6.6.4.1 o posteriores.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-921
Asunto	NUEVA VULNERABILIDAD EN NVIDIA CONTAINER TOOLKIT
Emisión	26/09/2024
CVE	CVE-2024-0132, CVE-2024-0133
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• NVIDIA Container Toolkit 1.16.1 y anteriores

Descripción

La más grave de ellas, CVE-2024-0132, es una vulnerabilidad de tiempo de comprobación, tiempo de uso (TOCTOU). Este fallo puede ser explotado cuando el kit de herramientas se utiliza con su configuración predeterminada, permitiendo que una imagen de contenedor especialmente diseñada obtenga acceso no autorizado al sistema de archivos host.

Una explotación exitosa puede llevar a graves consecuencias, incluyendo la ejecución remota de código, denegación de servicio, escalada de privilegios, divulgación de información y manipulación de datos. Esta vulnerabilidad ha recibido una calificación de gravedad crítica.

CVE-2024-0133 presenta un riesgo menos grave pero aún significativo. Un atacante puede crear archivos vacíos en el sistema de archivos del host a través de una imagen de contenedor manipulada. Aunque esta vulnerabilidad conduce principalmente a la manipulación de datos, ha sido calificada con una gravedad media.

Estas vulnerabilidades no afectan a los casos de uso en los que se utiliza la interfaz de dispositivo de contenedor (CDI). Sin embargo, para las configuraciones que dependen de los ajustes por defecto, el riesgo sigue siendo considerable.

NVIDIA ha instado a los usuarios a evaluar sus configuraciones específicas para comprender el impacto potencial. Para mitigar estos riesgos, NVIDIA recomienda actualizar a la versión 1.16.2 de Container Toolkit y a la versión 24.6.2 de NVIDIA GPU Operator. Estas actualizaciones solucionan las vulnerabilidades mediante la implementación de los parches necesarios que impiden su explotación.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-922
Asunto	NUEVA ACTUALIZACIÓN DE SEGURIDAD EN HPE ARUBA NETWORKING
Emisión	26/09/2024
CVE	CVE-2024-42505, CVE-2024-42506, CVE-2024-42507
Categoría	Actualización
Severidad	CRÍTICA

Servicios Afectados

• AOS-10.6.x.x: Versiones 10.6.0.2 e inferiores

• AOS-10.4.x.x: Versiones 10.4.1.3 e inferiores

• Instant AOS-8.12.x.x: Versiones 8.12.0.1 e inferiores

• Instant AOS-8.10.x.x: Versiones 8.10.0.13 e inferiores

Descripción

Las vulnerabilidades surgen de fallos de inyección de comandos en el servicio CLI subyacente, accesible a través del puerto UDP (8211) de PAPI (protocolo de gestión de puntos de acceso de Aruba). Los atacantes no autenticados pueden explotar estos defectos mediante el envío de paquetes especialmente diseñados, lo que lleva a la potencial ejecución remota de código con acceso privilegiado en los dispositivos afectados.

Además, varias versiones de software han llegado al final de su vida útil (EoSL) y ya no están cubiertas por este aviso. Por ello se recomienda encarecidamente a los clientes afectados que utilicen versiones EoSL, como AOS-10.5.x.x e Instant AOS-8.11.x.x, que actualicen inmediatamente a una versión compatible para garantizar la seguridad de sus sistemas.

En el momento de la publicación del aviso no se conocen discusiones públicas ni exploits dirigidos a estas vulnerabilidades específicas, pero los atacantes podrían desarrollar rápidamente código malicioso una vez que los detalles de la vulnerabilidad se difundan ampliamente.

Para solucionar por completo las vulnerabilidades, HPE Aruba Networking ha publicado versiones de software parcheadas para todos los dispositivos.

Actualización o Mitigación

• Actualizar a AOS-10.7.x.x: Versión 10.7.0.0 y superiores, AOS-10.6.x.x: Versión 10.6.0.3 y superiores, AOS-10.4.x.x: Versión 10.4.1.4 y superiores, Instant AOS-8.12.x.x: Versión 8.12.0.2 y superiores, Instant AOS-8.10.x.x: Versión 8.10.0.14 y superiores para mitigar las vulnerabilidades.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-924
Asunto	VULNERABILIDADES EN CUPS PODRÍAN PERMITIR LA EJECUCIÓN REMOTA DE CÓDIGO
Emisión	26/09/2024
CVE	Múltiples CVE's
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Todas las versiones de Red Hat Enterprise Linux (RHEL)

Descripción

Se han identificado varias vulnerabilidades críticas en el sistema de impresión CUPS, específicamente las catalogadas como CVE-2024-47076, CVE-2024-47175, CVE-2024-47176 y CVE-2024-47177. Estas vulnerabilidades permiten a los atacantes ejecutar código de manera remota en sistemas vulnerables, aunque no afectan a las configuraciones predeterminadas del software. CUPS, que significa Common UNIX Printing System, es una solución ampliamente utilizada en sistemas operativos Linux y otras plataformas Unix-like.

Un componente esencial de esta arquitectura es el componente cups-browsed, encargado de la detección y configuración automática de impresoras en la red local. Este servicio, cuando se encuentra habilitado, conectándose en el puerto UDP 631 y permite conexiones remotas para la creación de nuevas impresoras. Se demostró que un atacante podría crear una descripción de impresora maliciosa (PPD) que, al ser anunciada a un servicio cups-browsed expuesto, provocaría la instalación automática de dicha impresora en el sistema objetivo.

El vector de ataque se basa en que, una vez instalada la impresora maliciosa, el usuario imprima desde esta, lo que desencadenaría la ejecución de comandos maliciosos a través del filtro foomatic-rip. Este filtro es responsable de procesar los trabajos de impresión, lo que permite la inyección de código nocivo en el flujo de trabajo de impresión. Por lo tanto, la explotación de estas vulnerabilidades depende de una combinación de condiciones que incluyen la suplantación de impresoras y la interacción del usuario.

A pesar de que la ejecución remota de código (RCE) es potencialmente grave, el impacto real se considera limitado. Red Hat ha clasificado estas vulnerabilidades como de "importante" severidad en lugar de "crítica", debido a que el servicio cups-browsed generalmente no está habilitado por defecto y requiere que el sistema esté expuesto a conexiones UDP, lo cual es poco común en configuraciones de red seguras.

Actualización o Mitigación

• Los administradores de sistemas detengan y deshabiliten el servicio cups-browsed, utilizando comandos específicos que impiden su inicio automático.

• Los administradores pueden verificar el estado del servicio mediante comandos de sistema, asegurando que cualquier configuración vulnerable sea corregida antes de que se produzca una posible explotación.

Boletín	2024-925
Asunto	NUEVA FALLA DE SEGURIDAD CRITICA EN VLC
Emisión	27/09/2024
CVE	CVE-2024-46461
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Reproductor Multimedia VLC versión 3.0.20 y anteriores.

Descripción

La vulnerabilidad identificada fue catalogada como **CVE-2024-46461**, con una puntuación de CVSS de 8.0, el cual reside por un posible desbordamiento de enteros que puede activarse cuando VLC procesa un flujo MMS creado con fines malintencionados, ocasionando un posible bloqueo ejecución remota de código.

Según el equipo de VLC, la falla podría simplemente bloquear el programa, pero no descartan que se puedan combinar para filtrar información del usuario o ejecutar código de forma remota, asimismo mencionan que, la aleatorización del diseño del espacio de direcciones (ASLR) y la prevención de ejecución de datos (DEP), podrían ayudar a reducir la probabilidad de ejecución de código. También hacen mención de que una solución alterna seria que un usuario debería abstenerse de abrir transmisiones mms de terceros que no sean confiables o de contrario tener que deshabilitar los complementos del navegador VLC, sin embargo, el equipo trabajo en una versión del programa que solucionaría los inconvenientes.

Es importante resaltar que hasta la actualidad no se ha identificado un ataque real que haya explotado esta falla para ejecutar código, pero que esta si requiere aplicar la actualización.

Actualización o Mitigación

• Actualizar el reproductor multimedia VLC 3.0.21.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización

Boletín	2024-926
Asunto	NUEVAS FALLAS DE SEGURIDAD CRITICAS EN WHATSUP GOLD
Emisión	27/09/2024
CVE	Múltiples CVEs
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• WhatsUp Gold en versiones anteriores a la 24.0.1.

Descripción

Según el equipo de Progress Software las fallas identificadas plantean el acceso y el control no autorizados de la infraestructura de la red, asimismo poder interrumpir servicios y estarían afectando a todas las versiones de WhatsUp Gold anteriores a la 24.0.1. Las vulnerabilidades detectadas fueron:

CVE-2024-46909 con puntuación de CVSS de 9.8.

CVE-2024-8785 con puntuación de CVSS de CVSS 9.8, siendo una falla una falla crítica de ejecución remota de código no autenticado.

CVE-2024-46908 con puntuación de CVSS de CVSS 8.8.

CVE-2024-46907 con puntuación de CVSS de CVSS 8.8.

CVE-2024-46906 con puntuación de CVSS de CVSS 8.8.

CVE-2024-46905 con puntuación de CVSS de CVSS 8.8.

Por parte de Progress Software menciona que se encuentra en constante comunicación con sus clientes que usan el servicio de WhatsUp Gold, instando a actualizar sus entornos a la versión más reciente.

Actualización o Mitigación

• Actualizar WhatsUp Gold a la versión más reciente 24.0.1.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-928
Asunto	NUEVA VULNERABILIDAD DE HASHICORP VAULT
Emisión	28/09/2024
CVE	CVE-2024-759
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Vault Community Edition desde 1.7.7 hasta 1.17.5.

• Vault Enterprise desde 1.7.7 hasta 1.17.5, 1.16.9, 1.15.14.

Descripción

La vulnerabilidad **CVE-2024-759:** El campo valid_principals es utilizado por el servidor SSH para validar el certificado generado por Vault. En el contexto de la validación de certificados SSH, "principales válidos" puede ser una cadena que contenga cero o más principales. Cuando se establece en una cadena vacía o cero principales, el certificado es válido para cualquier principal del tipo especificado. Vault ahora proporciona una configuración allow_empty_principals para el motor de secretos SSH, con el valor predeterminado falso, para garantizar un valor predeterminado seguro y ayudar a preservar la compatibilidad con versiones anteriores.

Actualización o Mitigación

• Actualizar a Vault Community Edition 1.17.6.

• Actualizar a Vault Enterprise 1.17.6, 1.16.10 y 1.15.15.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-929
Asunto	NUEVAS VULNERABILIDADES EN WATCHGUARD
Emisión	28/09/2024
CVE	CVE-2024-6592, CVE-2024-6593
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Authentication gateway: Anterior a la versión 12.10.2.

• Windows single sign-on client: Anterior a la versión 12.7.

• MacOS Single Sign-On Client: Anterior a la versión 12.5.4.

Descripción

La vulnerabilidad **CVE-2024-6593**, permite a un ciberdelincuente con acceso a la red ejecutar comandos de gestión restringidos en el gateway de autenticación. Esto podría dar lugar a la recuperación de información confidencial del usuario, como nombres de usuario y membresías de grupos, o incluso a la manipulación de la configuración del agente. Sin embargo, es importante señalar que esta falla no se puede utilizar directamente para obtener credenciales de usuario.

La segunda vulnerabilidad **CVE-2024-6592**, implica una autorización incorrecta en el protocolo de comunicación entre la puerta de enlace de autenticación y el cliente de inicio de sesión único tanto en Windows como en MacOS. Esto permite a un ciberdelincuente falsificar las comunicaciones y potencialmente extraer nombres de usuario autenticados e información de grupo o incluso enviar datos arbitrarios de cuentas y grupos a la puerta de enlace de autenticación.

Actualización o Mitigación

• Actualizar Authentication Gateway a la versión 12.10.2 o posterior.

• Windows Single Sign-On Clients a la versión 12.7 o posterior.

• MacOS Single Sign-On Client a la versión 12.5.4 o posterior.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-930
Asunto	NUEVAS FALLAS DE SEGURIDAD CRITICAS EN WORDPRESS
Emisión	28/09/2024
CVE	Múltiples CVEs
Categoría	Vulnerabilidad
Severidad	CRÍTICA

Servicios Afectados

• Complemento Jupiter X Core de WordPress.

Descripción

La primera vulnerabilidad fue catalogada como **CVE-2024-7772**, con una puntuación de CVSS de 9.8, siendo una falla de puerta de acceso a la ejecución remota de código, así que el complemento es vulnerable a la carga de archivos arbitrarios debido a una validación de tipo de archivo mal gestionada en la función "validar" ocasionando que atacantes no autenticados carguen archivos arbitrarios en el servidor del sitio afectado, lo que puede hacer posible la ejecución remota de código.

La segunda vulnerabilidad fue catalogada como **CVE-2024-7781**, con una puntuación de CVSS de 8.1, siendo una falla de para evitar la autenticación y apoderarse de cuentas, esto se debe a una autenticación incorrecta a través del widget de inicio de sesión social, por lo cual, los atacantes podrían explotar la vulnerabilidad incluso si el elemento de inicio de sesión social se ha deshabilitado, siempre que se haya habilitado y utilizado previamente.

Por parte del proveedor, ya lanzo una versión parcheada, en la cual se solucionaron los inconvenientes, por lo que instan a usuarios a llevar a cabo la última actualización.

Actualización o Mitigación

• Actualizar el complemento Jupiter X Core a la última versión parcheada 4.7.8.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-933
Asunto	NUEVA VULNERABILIDAD EN UN DRIVER DE MICROSOFT
Emisión	29/09/2024
CVE	CVE-2024-45383, CVE-2024-38140
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Denominada como CVE-2024-45383, es una vulnerabilidad en el controlador de bus de audio de alta definición de Microsoft que podría permitir a un atacante provocar una denegación de servicio.

Este controlador es crucial para que el sistema operativo Windows se comunique con dispositivos de audio externos, incluidos los integrados en placas base o conectados a través de interfaces de audio HD. La vulnerabilidad surge del mal manejo de las peticiones IRP (I/O Request Packet) en la interfaz del driver.

Un atacante puede aprovecharse de ello enviando múltiples peticiones IRP Complete al controlador, provocando una denegación de servicio y forzando al sistema operativo a la "Pantalla azul de la muerte".

La otra vulnerabilidad es una corrupción de memoria en el servidor Pragmatic General Multicast del Kernel de Microsoft Windows 10.

Esta vulnerabilidad, CVE-2024-38140, puede ser activada por un paquete de red especialmente diseñado que accede a estructuras de memoria obsoletas, dando lugar a la corrupción de memoria. Un atacante puede explotar esta vulnerabilidad enviando una secuencia de paquetes maliciosos.

Aunque se descubrió este problema de forma independiente y se informó a Microsoft, la empresa ya lo había identificado internamente antes de la publicación del parche a principios de este año.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización

Boletín	2024-934
Asunto	ACTUALIZACION PARA FALLA DE SEGURIDAD CRITICA EN KERNEL DE LINUX
Emisión	30/09/2024
CVE	CVE-2024-26808
Categoría	Actualización
Severidad	CRÍTICA

Servicios Afectados

• Kernel de Linux en versiones desde 5.9 hasta la 6.6.

Descripción

Según los investigadores, la falla de seguridad se origina por el manejo inadecuado del procesamiento de paquetes de red, conduciendo a una posibilidad de acceso no autorizado a la memoria.

La vulnerabilidad identificada fue catalogada como **CVE-2024-26808**, siendo una falla por el uso posterior a la liberación dentro del kernel de Linux Netfilter, el cual es un marco integral de la pila de redes de Linux, para ello Netfilter proporciona operaciones de red esenciales como por ejemplo el filtrado de paquetes, traducción de direcciones de red (NAT) o reenvío de puertos.

Asimismo, los investigadores mencionan que ciberdelincuentes podrían aprovechar la falla para escalar privilegios y, potencialmente, obtener acceso root al sistema afectado, mediante pruebas de concepto, ya que aseguran que el exploit aprovecha las sobrescrituras de caché cruzadas, donde los datos de un área de memoria se utilizan para corromper otra, y el control preciso sobre los búferes de canalización para manipular las estructuras del núcleo.

La divulgación del código de explotación de prueba de concepto (PoC) para la falla en mención ya se había publicado por GitHub, aumentando la probabilidad de explotación en la red. Sin embargo, debido al uso generalizado del kernel de Linux en entornos empresariales, centros de datos y plataformas en la nube, el equipo de desarrollo de Linux anunció un parche que soluciona el problema, por lo que instan a usuarios, actualizar a la última versión el kernel, para mitigar el riesgo de seguridad.

Actualización o Mitigación

• Actualizar a la última versión el kernel de Linux.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización

Boletín	2024-935
Asunto	NUEVAS VULNERABILIDADES EN PHP
Emisión	30/09/2024
CVE	CVE-2024-9026, El CVE-2024-8927, El CVE-2024-8926, El CVE-2024-8925
Categoría	Vulnerabilidad
Severidad	ALTA

Servicios Afectados

• Versiones de PHP anteriores a la 8.1.30

• Versiones de PHP anteriores a la 8.2.24

• Versiones de PHP anteriores a la 8.3.12

Descripción

El CVE-2024-9026 es vulnerabilidad que permitiría la manipulación potencial de registros en PHP-FPM, permitiendo a los atacantes insertar caracteres extraños o eliminar hasta 4 caracteres de las entradas de registro. Esto puede dificultar la respuesta a incidentes y las investigaciones forenses.

El CVE-2024-8927 es una vulnerabilidad donde los atacantes pueden aprovechar este fallo para saltarse las restricciones impuestas por la configuración de cgi.force_redirect, lo que puede dar lugar a la inclusión de archivos arbitrarios en determinadas configuraciones. Esto puede comprometer datos sensibles y permitir accesos no autorizados.

El CVE-2024-8926 sería una vulnerabilidad que elude una corrección anterior (CVE-2024-4577) bajo configuraciones específicas y no estándar de páginas de código de Windows. Aunque es poco probable que se produzca en entornos reales, subraya la importancia de abordar incluso las vulnerabilidades aparentemente menores.

El CVE-2024-8925 es un fallo en el análisis sintáctico de datos de formularios multiparte que puede provocar que no se procesen datos legítimos, violando la integridad de los datos. Los atacantes pueden aprovecharse de ello para excluir partes de datos legítimos en determinadas condiciones.

Actualización o Mitigación

• Actualizar a la versión recomendada por el proveedor para mitigar la vulnerabilidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización

Amenazas

Boletín	2024-877
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE MEDUSA
Emisión	16/09/2024
CVE	No
Categoría	Ransomware
Severidad	CRÍTICA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Esta estrategia inusual ha amplificado su impacto, con actualizaciones frecuentes en su blog y canal de Telegram que muestran su rápido ritmo de ataques y tácticas para presionar a las víctimas.

El grupo de ransomware opera un modelo RaaS, dirigido a diversos sectores, como el sanitario, la fabricación y la educación. Además, ha lanzado ataques a nivel mundial, con un aumento significativo de víctimas en 2024.

Mantiene un blog donde publica información sobre sus objetivos y las peticiones de rescate. Las víctimas pueden elegir pagar por los datos robados, su eliminación o una ampliación del plazo.

Este grupo mantiene una inusual presencia en línea combinando actividades en la dark web y la surface web. El sitio accesible incluye descargos de responsabilidad para evitar repercusiones legales, pero dirige a los usuarios a un canal de Telegram, también vinculado a su blog oficial.

El grupo de ransomware utiliza Telegram para comunicarse y compartir información, ya que su canal presenta filtraciones de datos, enlaces onion y descripciones positivas del grupo, una comunicación abierta que plantea riesgos, porque permite la infiltración de grupos de seguridad.

Un incidente reciente expuso el token de acceso al almacenamiento en la nube de Medusa a través de un archivo de configuración, lo que permitió a un usuario ver la información comprometida de las víctimas y tomar contramedidas, lo que pone de relieve la vulnerabilidad de las operaciones de ransomware cuando una comunicación web clara expone su infraestructura.

Este grupo tendría como objetivos a sistemas vulnerables a través de ataques de inyección SQL y aprovecha las herramientas RMM comprometidas para ganar persistencia y movimiento lateral mediante el aprovechamiento de secuencias de comandos PowerShell para ejecutar comandos maliciosos, cifrar archivos y filtrar datos.

Para eludir la detección, Medusa emplea técnicas como la evasión antimalware y la eliminación de copias de seguridad. La nota del ransomware exige el pago de un rescate y amenaza con liberar los datos robados si no se cumple.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2024-879
Asunto	EXPLOTACIÓN DE UNA VULNERABILIDAD EN WINDOWS POR EL GRUPO VOID BANSHEE APT
Emisión	16/09/2024
CVE	CVE-2024-43461
Categoría	Ataque Cibernético
Severidad	CRÍTICA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Se identificó que la vulnerabilidad de suplantación de identidad en MSHTML de Windows, rastreada como CVE-2024-43461, fue explotada previamente en ataques antes de ser corregida. Inicialmente, cuando Microsoft reveló esta vulnerabilidad durante el Patch Tuesday de septiembre de 2024, no había sido marcada como explotada previamente. Sin embargo, el viernes, Microsoft actualizó el aviso de CVE-2024-43461 para indicar que la falla ya había sido utilizada en ataques antes de que se lanzara el parche correspondiente.

Esta vulnerabilidad fue descubierta por un investigador de seguridad, quien reveló que el grupo de ciberespionaje Void Banshee explotó esta vulnerabilidad en ataques de 0-day para instalar malware diseñado para robar información. Void Banshee, un grupo APT rastreado por investigadores, ha estado activo en ataques dirigidos a organizaciones en América del Norte, Europa y el sudeste asiático, principalmente con fines de robo de datos y ganancia financiera.

El CVE-2024-43461 es una de las dos vulnerabilidades utilizadas en una cadena de ataques que también incluyó el CVE-2024-38112. Ambos fallos fueron explotados para infectar dispositivos con el malware Atlantida, un info-stealer capaz de robar contraseñas, cookies de autenticación y carteras de criptomonedas. En particular, la vulnerabilidad CVE-2024-38112 permitía que archivos de acceso directo maliciosos forzaran a Windows a abrir sitios web en Internet Explorer, facilitando la descarga de archivos HTA maliciosos que instalaban el malware.

La vulnerabilidad CVE-2024-43461 jugaba un papel clave en ocultar la verdadera naturaleza de estos archivos HTA. Mediante el uso de caracteres de espacio en blanco en braille, los atacantes ocultaban la extensión ".hta" del archivo, haciendo que pareciera un archivo PDF en las ventanas emergentes de Windows. Aunque el parche corrige esta falla mostrando la extensión real ".hta" en las alertas del sistema, los caracteres de espacio en blanco aún pueden confundir a los usuarios, haciéndoles creer que se trata de un archivo PDF legítimo.

Actualización o Mitigación

• Aplicar de inmediato las actualizaciones de seguridad proporcionadas por Microsoft para corregir las vulnerabilidades.

• Implementar soluciones de seguridad avanzadas, como EDR y firewalls, para detectar y prevenir el malware Atlantida y otras amenazas similares.

• Implementar Autenticación Multifactor (MFA) en todas las cuentas críticas para prevenir accesos no autorizados.

Boletín	2024-881
Asunto	CIBERDELINCUENTES DISTRIBUYEN REMCOS RAT A TRAVÉS DE ARCHIVOS EXCEL
Emisión	17/09/2024
CVE	CVE-2017-0199
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

El ataque comienza con un correo phishing que contiene un archivo de Excel cifrado que parece protegido, induciendo a la interacción del usuario. Al abrir el archivo, explota la CVE-2017-0199 para ejecutar objetos OLE incrustados descargando un archivo HTA malicioso desde una URL.

A continuación, este archivo ejecuta comandos PowerShell con parámetros codificados en base64 que ayudan a recuperar un VBScript de otra url. Este contiene datos ofuscados que, al ser procesados por PowerShell, generan procesos PowerShell adicionales.

Estos procesos descargan un archivo JPEG que contiene el payload final. El ataque inyecta una variante sin archivos de Remcos RAT en un proceso legítimo de Windows.

En esta campaña, los atacantes demostraron sus tácticas de evasión, ya que se dirigieron principalmente a los sectores de Gobierno, Industria, TI y Banca en Bélgica, Japón, EE.UU., Corea del Sur, Canadá, Alemania y Australia.

Este formaría parte de una tendencia que incluye ataques similares que despliegan malware como RevengeRAT, SnakeKeylogger, GuLoader, AgentTesla y FormBook.

El método en varias fases emplea técnicas como T1221 (Template Injection) y T1059.001 (Visual Basic Scripting) para eludir las medidas de seguridad, lo que pone de relieve la complejidad cambiante de las ciberamenazas que aprovechan documentos aparentemente inofensivos para distribuir payloads.

En resumen, el ataque comienza con un archivo JPEG que contiene una dnlib[.]dll codificada en base64, una biblioteca .NET de código abierto para la manipulación de ensamblados.

Esta dll se descodifica y se carga directamente en memoria a través de System[.]Reflection[.]Assembly, una clase .NET que permite realizar operaciones de ensamblado en tiempo de ejecución. A continuación, PowerShell descarga un archivo de texto con datos codificados en base64 desde una URL maliciosa. Estos datos son descodificados y procesados por la dnlibdll cargada para generar un ensamblado .NET en memoria de Remcos RAT.

Luego, la RAT se inyecta en el proceso legítimo de Windows 'RegAsm[.]exe' para su ejecución, y este proceso deja rastros mínimos de comportamientos asociados a Remcos. El malware establece la persistencia a través de la inyección del proceso que asegura el acceso continuo del atacante.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2024-887
Asunto	ATAQUES DE PHISHING DE COREA DEL NORTE UTILIZAN EL BACKDOOR MISTPEN
Emisión	18/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Se ha observado a un grupo de ciberespionaje vinculado a Corea del Norte utilizando señuelos de phishing relacionados con ofertas de trabajo para atacar a posibles víctimas en los sectores de energía y aeroespacial. Este grupo ha desplegado un backdoor previamente no documentado, denominado MISTPEN, como parte de sus ataques. La actividad de este grupo es rastreada por investigadores bajo el nombre UNC2970, el cual presenta similitudes con TEMP.Hermit, un grupo que también es conocido como Lazarus Group o Diamond Sleet (anteriormente llamado Zinc).

Este actor de amenazas tiene un largo historial de atacar a instituciones gubernamentales, de defensa, telecomunicaciones y financieras en todo el mundo desde al menos 2013, con el objetivo de recopilar inteligencia estratégica que beneficie a los intereses de Corea del Norte. El grupo está afiliado al Buró General de Reconocimiento (RGB), la agencia de inteligencia militar de Corea del Norte.

UNC2970 ha sido observado apuntando a entidades ubicadas en países como Estados Unidos, Reino Unido, Países Bajos, Chipre, Suecia, Alemania, Singapur, Hong Kong y Australia. Los ataques de este grupo se presentan bajo la apariencia de ofertas laborales, haciéndose pasar por reclutadores de empresas destacadas. Según los investigadores, los atacantes ajustan y modifican descripciones de trabajo según el perfil de sus objetivos, enfocándose en empleados de nivel alto o gerencial. Esto sugiere que buscan obtener acceso a información confidencial y sensible, típicamente restringida a empleados de alto nivel.

El ataque, conocido como "Operación Dream Job", utiliza señuelos de spear-phishing para atraer a las víctimas mediante correos electrónicos y WhatsApp, con el fin de generar confianza antes de enviar un archivo ZIP malicioso disfrazado como una descripción de trabajo. En un giro interesante, el archivo PDF con la supuesta oferta laboral solo puede abrirse con una versión troyanizada de una aplicación legítima llamada Sumatra PDF, incluida dentro del archivo ZIP, que se utiliza para entregar el malware MISTPEN a través de un lanzador conocido como BURNBOOK.

Es importante destacar que este ataque no involucra una vulnerabilidad en el software Sumatra PDF ni un ataque a la cadena de suministro. Más bien, se emplea una versión antigua del lector de PDF que ha sido reutilizada para activar la cadena de infección. Este método ha sido utilizado por el grupo desde 2022, usando software de código abierto como PuTTY, KiTTY, TightVNC, y Sumatra PDF, entre otros.

Los atacantes instruyen a las víctimas para que abran el archivo PDF con el visor PDF incluido en el ZIP, lo que activa la ejecución de un archivo DLL malicioso, un lanzador en C/C++ llamado BURNBOOK.

Este archivo actúa como dropper para un DLL incrustado llamado "wtsapi32.dll", el cual es rastreado como TEARPAGE y se encarga de ejecutar el backdoor MISTPEN después de que el sistema se reinicia.

MISTPEN es una versión troyanizada de un plugin legítimo de Notepad++ llamado "binhex.dll", que contiene una puerta trasera. El loader TEARPAGE, incrustado dentro de BURNBOOK, es responsable de descifrar y ejecutar MISTPEN. Este implante ligero, escrito en C, está diseñado para descargar y ejecutar archivos ejecutables portátiles (PE) desde un servidor de comando y control (C2). MISTPEN se comunica a través de HTTP con URLs de Microsoft Graph.

Además, los investigadores han descubierto que tanto BURNBOOK como MISTPEN han sido iterativamente mejorados para añadir nuevas capacidades y evadir la detección. Se han encontrado muestras más antiguas de MISTPEN utilizando sitios web comprometidos de WordPress como dominios de C2. Los investigadores señalan que los atacantes han implementado nuevas funciones en su malware, incluyendo una verificación de conectividad de red para dificultar el análisis de las muestras.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-893
Asunto	CAMPAÑA DE DISTRIBUCIÓN DE LUMMA STEALER UTILIZA REPOSITORIOS DE GITHUB PARA PROPAGAR MALWARE
Emisión	19/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Se ha detectado una campaña maliciosa que aprovecha los repositorios de GitHub para distribuir el malware Lumma Stealer, diseñado para robar contraseñas. Esta campaña se dirige a usuarios que frecuentan proyectos de código abierto o que están suscritos a notificaciones por correo electrónico de estos repositorios.

El ataque comienza cuando un usuario malicioso de GitHub crea un nuevo "issue" en un repositorio, alegando falsamente que el proyecto contiene una "vulnerabilidad de seguridad". En este mensaje, se insta a los usuarios a visitar un dominio falso llamado "GitHub Scanner", que no tiene relación alguna con GitHub. Este sitio engaña a las víctimas para que instalen malware en sus dispositivos Windows.

Lo que hace que esta campaña sea más convincente es que las notificaciones que reciben los usuarios provienen de servidores legítimos de GitHub, lo que aumenta la credibilidad del mensaje. Los correos electrónicos se envían desde la dirección oficial de GitHub, notifications@github.com, y están firmados por el equipo de seguridad de GitHub.

Al visitar el dominio github-scanner[.]com, los usuarios son recibidos por un captcha falso que les solicita verificar que no son robots. Sin embargo, al hacer clic en "I'm not a robot", un código JavaScript copia un código malicioso en el portapapeles de la víctima. Luego, se instruye al usuario a ejecutar este código mediante el comando "Ejecutar" en Windows, lo que descarga y ejecuta un archivo malicioso llamado 'SysSetup.exe', que contiene el malware Lumma Stealer.

Este malware es capaz de robar credenciales, cookies de autenticación e historiales de navegación de los navegadores instalados. Además, puede robar billeteras de criptomonedas y archivos sensibles del dispositivo infectado. El ataque se propaga mediante la funcionalidad de "Issues" de GitHub, aprovechando que las notificaciones por correo se envían automáticamente a los suscriptores de los repositorios afectados.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Boletín	2024-896
Asunto	SAMBASPY ESTARÍA UTILIZANDO ARCHIVOS PDF PARA REALIZAR ATAQUES
Emisión	20/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Los atacantes utilizaron un correo electrónico de spear phishing con una factura falsa de una empresa inmobiliaria italiana para engañar a los usuarios e inducirlo a hacer clic en un enlace malicioso. Este redirigía a los usuarios a un sitio web que parecía un sitio web legítimo de almacenamiento de facturas, pero luego enviaba a los usuarios que utilizaban Edge, Firefox o Chrome a una URL maliciosa de OneDrive. La URL redirigía a los usuarios a un archivo JAR malicioso alojado en MediaFire.

Este malware emplea un proceso de entrega en dos fases, en el que el descargador inicial verifica que no se está ejecutando en un entorno virtualizado y se asegura de que la configuración regional del sistema es italiana. Si las comprobaciones se superan, recupera el payload final, probablemente otro ejecutable malicioso.

El dropper, incrustado en los recursos del downloader, realiza verificaciones idénticas, pero transporta él mismo payload, lo que elimina la necesidad de comunicación adicional a través de la red. Una vez realizadas las comprobaciones, tanto el descargador como el dropper ejecutan el payload incrustada, completando la infección.

SambaSpy, una RAT basada en Java, emplea Zelix KlassMaster para ofuscar sus cadenas, nombres de clases y métodos, dificultando el análisis y la detección. Su amplio conjunto de funciones incluye la gestión de procesos y del sistema de archivos, transferencias de archivos, control de cámaras web, registro de pulsaciones de teclas, manipulación del portapapeles, captura de pantallas, control remoto del escritorio, robo de contraseñas, carga de plugins, ejecución remota de shell e interacción con la víctima.

El mecanismo de carga de plugins implica la carga de clases a través de URLClassLoader para acceder a los archivos descargados y la posterior adición de URL. El RAT emplea la biblioteca JNativeHook para capturar y transmitir pulsaciones de teclas a un servidor de comando y control.

Además, aprovecha el Abstract Window Toolkit de Java para robar o manipular el contenido del portapapeles. La RAT es capaz de extraer credenciales de varios navegadores web, como Chrome, Edge, Opera, Brave, Iridium y Vivaldi. SambaSpy implementa un sistema de control remoto personalizado, utilizando la clase Robot para simular acciones de ratón y teclado y la clase GraphicsDevice para proporcionar una representación visual de la pantalla de la víctima al atacante.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2024-901
Asunto	EL GRUPO HACKTIVISTA TWELVE ATACA A ENTIDADES RUSAS
Emisión	21/09/2024
CVE	CVE-2021-21972, CVE-2021-22005
Categoría	Ataque Cibernético
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

El grupo hacktivista conocido como Twelve ha realizado ataques cibernéticos dirigidos a entidades rusas. Desde su formación en abril de 2023, tras el inicio de la guerra entre Rusia y Ucrania, Twelve ha demostrado una inclinación por utilizar herramientas de código abierto y técnicas bien documentadas para infiltrarse en las redes de sus víctimas. A diferencia de otros grupos de ransomware que buscan obtener beneficios económicos, Twelve se centra en la destrucción de infraestructuras y el cifrado de datos, impidiendo así la recuperación de la información afectada.

Los métodos de acceso inicial de Twelve implican el abuso de cuentas locales o de dominio válidas, seguido de la utilización del Protocolo de Escritorio Remoto (RDP) para facilitar el movimiento lateral dentro de la red comprometida. Además, han explotado vulnerabilidades conocidas, como CVE-2021-21972 y CVE-2021-22005 en VMware vCenter, para implementar web shells y puertas traseras como FaceFish. Este enfoque subraya la importancia de una adecuada gestión de la seguridad y la aplicación de parches en las organizaciones objetivo.

Entre las herramientas utilizadas por Twelve se encuentran soluciones como Cobalt Strike, Mimikatz y PowerShell, que les permiten realizar actividades de robo de credenciales, descubrimiento de red y escalación de privilegios. La inclusión de PHP web shells y la utilización de conexiones RDP a través de túneles ngrok son estrategias clave para mantener el control sobre las máquinas comprometidas. Asimismo, emplean scripts de PowerShell para deshabilitar procesos de software de seguridad, lo que les facilita la ejecución de sus ataques sin ser detectados.

El desenlace de estos ataques suele implicar la recopilación y exfiltración de información sensible, a menudo utilizando servicios de transferencia de archivos como DropMeFiles. En la fase final, utilizan una variante de ransomware, similar a LockBit 3.0, para cifrar los datos de la víctima, y un wiper que actúa de manera análoga al malware Shamoon, reescribiendo el registro de arranque maestro (MBR) y sobrescribiendo los contenidos de los archivos. Esto no solo imposibilita la recuperación, sino que también destruye de forma irreversible la información.

La relación observada entre Twelve y el grupo de ransomware DARKSTAR destaca la complejidad y diversidad de las amenazas cibernéticas modernas, donde diferentes actores pueden compartir tácticas y herramientas, pero con objetivos claramente distintos.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2024-903
Asunto	CIBERDELINCUENTES ESTARÍAN UTILIZANDO MALWARE SUPERSHELL PARA ATACAR SERVIDORES SSH
Emisión	22/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Servidor SSH

Descripción

Investigadores descubrieron que el ataque se ha dirigido a servidores Linux SSH mal gestionados y poco seguros en los que los ciberdelincuentes instalaron el malware Supershell.

Este programa malicioso es compatible con las principales plataformas (Windows, Linux y Android) y desarrollado por un ciberdelincuente de habla china que utiliza el lenguaje de programación Go.

Su función principal es una shell inversa que permite a los atacantes controlar remotamente los sistemas infectados. Es probable que el ataque se llevara a cabo por etapas, en las que se comprometieron varios sistemas y se instaló un escáner, y luego se intentaron ataques de diccionario desde varias direcciones IP para obtener acceso no autorizado.

Una vez conseguida la intrusión, el atacante ejecutó comandos específicos para instalar directamente “Supershell” o desplegar un “script de Shell” que actúa como loader.

El malware se distribuyó tanto a través de servidores web como de servidores FTP, lo que contribuye a aumentar su alcance y no solo eso, sino que también dificultaría su detección.

El backdoor Supershell puede identificarse a través de sus strings internas, su comportamiento y su proceso de ejecución, ya que se trata de un tipo de malware dirigido a sistemas Linux vulnerables.

Suele instalarse junto a otros programas maliciosos como XMRig o bots DDoS como ShellBot y Tsunami. La función principal de Supershell es tomar el control del dispositivo, permitiendo a los atacantes controlar remotamente los servidores Linux SSH comprometidos. Aunque la instalación inicial se centra en establecer un backdoor, su objetivo real es minar criptomoneda.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-906
Asunto	NUEVO MALWARE PONDRAT
Emisión	23/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Linux, macOS

Descripción

Este malware se considera una versión más ligera de POOLRAT (también conocido como SIMPLESEA), un backdoor para macOS que se ha atribuido previamente al Grupo Lazarus y desplegado en ataques relacionados con el compromiso de la cadena de suministro de una compañía el año pasado.

Algunos de estos ataques forman parte de una campaña de ciberataque persistente denominada como 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 que están detrás de esta campaña subieron varios paquetes Python a PyPI, un popular repositorio de paquetes Python de código abierto.

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 endpoints de los desarrolladores y, posteriormente, obtener acceso a los endpoints de los clientes de los proveedores, como se ha observado en incidentes anteriores.

La lista de paquetes maliciosos, ahora eliminados del repositorio PyPI, es la siguiente: real-ids, coloredtxt, beautifultext y minisound.

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

PondRAT, como una versión reducida de POOLRAT, permitiría cargar y descargar archivos, pausar operaciones durante un intervalo de tiempo predefinido y ejecutar comandos arbitrarios.

La suplantación de paquetes Python de apariencia legítima en múltiples sistemas operativos supone un riesgo significativo para las organizaciones. La instalación exitosa de paquetes maliciosos de terceros puede resultar en una infección de malware que comprometa toda una red.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Boletín	2024-907
Asunto	CAMPAÑAS GLOBALES DE MALWARE DIRIGIDAS POR MARKO POLO
Emisión	23/09/2024
CVE	No
Categoría	Ataque Cibernético
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows, macOS

Descripción

Se ha descubierto una operación masiva de malware tipo infostealer, la cual abarca más de treinta campañas dirigidas a una amplia gama de demografías y plataformas de sistemas. Esta operación ha sido atribuida a un grupo de ciberdelincuentes conocido como "Marko Polo". Los actores de la amenaza utilizan diversos canales de distribución, como malvertising, spearphishing y suplantación de marcas en sectores como el gaming online, las criptomonedas y el software, para propagar más de 50 tipos de malware. Entre los principales se encuentran AMOS, Stealc y Rhadamanthys.

De acuerdo con los investigadores de seguridad, que han estado monitoreando la operación de Marko Polo, esta campaña de malware ha afectado a miles de víctimas, lo que podría traducirse en pérdidas financieras potenciales de varios millones de dólares. Se estima que decenas de miles de dispositivos han sido comprometidos a nivel global, exponiendo datos sensibles tanto personales como corporativos.

Los delincuentes detrás de Marko Polo centran sus esfuerzos en objetivos de alto valor, como influenciadores de criptomonedas, gamers y desarrolladores de software, a quienes llegan principalmente mediante spearphishing a través de mensajes directos en redes sociales. Las víctimas son engañadas para descargar software malicioso haciéndoles creer que se trata de ofertas laborales legítimas o colaboraciones en proyectos.

Algunas de las marcas suplantadas por los atacantes incluyen juegos como Fortnite, Party Icon, RuneScape y Rise Online World, además de plataformas de productividad como Zoom y criptomonedas como PeerMe. El grupo también crea marcas ficticias, como Vortax/Vorion y VDeck (software de reuniones), Wasper y PDFUnity (plataformas de colaboración), SpectraRoom (comunicaciones en cripto) y NightVerse (juego web3).

Marko Polo utiliza una amplia variedad de herramientas para sus ataques multiplataforma y multivectoriales. En Windows, emplean HijackLoader para distribuir malware como Stealc, diseñado para robar datos de navegadores y aplicaciones de billeteras criptográficas, o Rhadamanthys, que tiene un enfoque más especializado y apunta a una amplia gama de aplicaciones y tipos de datos. Este último ha evolucionado para desviar pagos en criptomonedas hacia las carteras de los atacantes y evadir la protección de Windows Defender.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2024-908
Asunto	INCIDENTE DE CIBERSEGURIDAD AFECTA SISTEMAS DE MONEYGRAM
Emisión	23/09/2024
CVE	No
Categoría	Actualización
Severidad	ALTA

Servicios Afectados

• MoneyGram

Descripción

El 21 de septiembre, MoneyGram informó a través de su cuenta en X (anteriormente Twitter) que estaban experimentando una interrupción en la red que afectaba la conectividad de varios de sus sistemas. Mencionaron que estaban trabajando para comprender mejor la naturaleza y el alcance del problema. Sin embargo, el 23 de septiembre, MoneyGram comunicó por el mismo medio que se había identificado un incidente de ciberseguridad que comprometió algunos de sus sistemas. Tras la detección, iniciaron las investigaciones correspondientes y procedieron a la desconexión proactiva de los sistemas afectados, lo que agravó los problemas de conectividad.

MoneyGram no ha proporcionado detalles sobre la naturaleza específica del incidente ni ha mencionado al grupo de ciberdelincuentes responsable. Continuaremos monitoreando esta situación y mantendremos a nuestros clientes informados sobre cualquier actualización relevante.

Actualización o Mitigación

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-912
Asunto	MALLOX RANSOMWARE ADOPTA CÓDIGO DE KRYPTINA PARA ATACAR SISTEMAS LINUX
Emisión	24/09/2024
CVE	CVE-2024-21338
Categoría	Ransomware
Severidad	CRÍTICA

Servicios Afectados

• Sistemas operativos Windows, Sistemas operativos Linux, VMWare ESXi

Descripción

Un afiliado de la operación de Ransomware Mallox, también conocido como TargetCompany, fue detectado utilizando una versión ligeramente modificada del Ransomware Kryptina para atacar sistemas Linux. Según un informe, esta versión es independiente de otras variantes de Mallox que también apuntan a Linux, como la descrita en junio por investigadores, lo que refleja un cambio en las tácticas del ecosistema del Ransomware.

Este hallazgo marca una evolución significativa para la operación de Mallox, que previamente se centraba exclusivamente en sistemas Windows. Ahora, también están dirigiendo sus ataques hacia sistemas Linux y VMWare ESXi, lo que amplía el rango de sus objetivos y aumenta el nivel de amenaza.

Kryptina, lanzada como una plataforma de Ransomware como servicio (RaaS) de bajo costo en 2023, no logró captar la atención en la comunidad cibercriminal. Sin embargo, en febrero de 2024, su código fuente fue filtrado gratuitamente en foros de hacking por un actor bajo el alias "Corlys". Esta filtración permitió que diferentes actores de Ransomware, incluido un afiliado de Mallox, adquirieran el código y lo adaptaran para sus operaciones.

Los investigadores descubrieron que el código de Kryptina fue utilizado para construir cargas maliciosas de Mallox bajo el nombre "Mallox Linux 1.0". Esta variante rebrandeada utiliza el código central de Kryptina, incluyendo el mismo mecanismo de cifrado AES-256-CBC, las rutinas de descifrado y las mismas herramientas de configuración. Los cambios realizados por los afiliados de Mallox fueron superficiales, limitándose a modificar el nombre, eliminar las referencias a Kryptina en las notas de rescate y ajustar la documentación, dejando intacta la funcionalidad original.

Además de la variante Mallox Linux 1.0, en el servidor del actor de amenazas se encontraron otras herramientas, como una utilidad legítima de Kaspersky para restablecer contraseñas (KLAPR.BAT), un exploit para la vulnerabilidad CVE-2024-21338 (una falla de escalamiento de privilegios en Windows 10 y 11), scripts de PowerShell para escalamiento de privilegios, y archivos de imagen de disco que contienen cargas de Mallox. También se hallaron carpetas con datos de posibles víctimas.

Aún no se ha determinado si esta nueva variante de Mallox Linux 1.0 está siendo utilizada por un solo afiliado, múltiples afiliados o por todos los operadores de Mallox en conjunto con otras variantes.

Actualización o Mitigación

• Implementar autenticación robusta, como autenticación de dos factores o autenticación basada en tokens, en lugar de depender únicamente de credenciales de usuario y contraseñas.

Boletín	2024-913
Asunto	MALWARE OCTO ESTARÍA SUPLANTANDO NORDVPN Y GOOGLE CHROME
Emisión	24/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Android

Descripción

La primera versión de Octo se observó en 2022 en falsas aplicaciones de limpieza en Google Play. Entre otras cosas, el malware permitiría el keylogging, la navegación en el dispositivo, la interceptación de SMS y notificaciones push, el bloqueo de la pantalla del dispositivo, el silenciamiento del sonido, el lanzamiento arbitrario de aplicaciones y el uso de dispositivos infectados para la distribución de SMS.

Los investigadores informaron que el código de Octo se habría filtrado este año, lo que provocó que aparecieran múltiples variantes del malware. Tras estos acontecimientos, el diseñador anunció Octo2, probablemente como un intento de lanzar una versión mejorada y despertar el interés de los ciberdelincuentes.

Las campañas que actualmente despliegan Octo2 se centran en Italia, Polonia, Moldavia y Hungría. Sin embargo, dado que la plataforma Octo Malware-as-a-Service (MaaS) ha facilitado anteriormente ataques en todo el mundo, incluidos Estados Unidos, Canadá, Australia y Oriente Medio, es probable que pronto veamos campañas de Octo2 en otras regiones.

En las operaciones europeas, los atacantes utilizan aplicaciones falsas de NordVPN y Google Chrome, así como una aplicación Europe Enterprise, que probablemente sea un señuelo utilizado en ataques dirigidos. Octo2 utiliza el servicio Zombider para añadir el payload en estos APKs, eludiendo las restricciones de seguridad de Android 13 (y posteriores).

En primer lugar, el autor del malware introdujo un nuevo ajuste de baja calidad en el módulo de la herramienta de acceso remoto (RAT) llamado “SHIT_QUALITY” que reduce las transmisiones de datos al mínimo, permitiendo una conectividad más fiable cuando las velocidades de conexión a Internet son deficientes.

Octo2 también descifra su payload utilizando código nativo y complica el análisis cargando dinámicamente bibliotecas adicionales durante la ejecución, lo que mejora aún más su capacidad de evasión.

Por último, Octo2 introduce un sistema de dominio C2 basado en DGA que permite a los operadores actualizar y cambiar rápidamente a nuevos servidores C2, haciendo ineficaces las listas de bloqueo y mejorando la resistencia frente a los intentos de desmantelamiento de los servidores.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2024-916
Asunto	NUEVA CAMPAÑA DE PHISHING APUNTA A EMPRESAS DE TRANSPORTE Y LOGÍSTICA
Emisión	25/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Una nueva campaña de phishing está dirigida a empresas de transporte y logística en América del Norte, entregando una variedad de programas maliciosos, como ladrones de información (stealers) y troyanos de acceso remoto (RATs). Según los investigadores, esta campaña utiliza cuentas de correo electrónico legítimas comprometidas pertenecientes a empresas de transporte y envío, infiltrando contenido malicioso en conversaciones de correo electrónico ya existentes. Hasta 15 cuentas de correo electrónico comprometidas han sido identificadas, pero aún no está claro cómo fueron vulneradas ni quién está detrás de los ataques.

Entre mayo y julio de 2024, la campaña distribuyó principalmente los malware Lumma Stealer, StealC y NetSupport. Sin embargo, en agosto de 2024, los atacantes cambiaron sus tácticas, empleando nueva infraestructura y técnicas de entrega, además de añadir nuevos programas maliciosos como DanaBot y Arechclient2. Los ataques incluyen el envío de mensajes con archivos adjuntos de acceso directo a internet (.URL) o enlaces a Google Drive que conducen a un archivo .URL. Al abrirse, este archivo utiliza el protocolo Server Message Block (SMB) para descargar la siguiente fase del malware desde un recurso remoto.

Algunas variantes de la campaña en agosto de 2024 también emplearon la técnica llamada ClickFix, donde los atacantes engañan a las víctimas para que descarguen el malware DanaBot bajo el pretexto de solucionar un problema con la visualización de documentos en el navegador. Esta técnica pide a los usuarios que copien y peguen un script PowerShell codificado en Base64 en la terminal, lo que desencadena el proceso de infección.

Los ataques han suplantado a software legítimo como Samsara, AMB Logistic y Astra TMS, que son utilizados exclusivamente en la gestión de operaciones de transporte y flotas. Esto sugiere que los atacantes investigan las operaciones de las empresas antes de lanzar las campañas, haciéndolas más específicas y efectivas.

Este escenario se presenta en medio de la proliferación de diversos tipos de malware diseñados para robar información, como Angry Stealer, BLX Stealer, Luxy, Poseidon y otros. Además, ha surgido una nueva versión del troyano RomCom RAT, llamada SnipBot, que se distribuye a través de enlaces fraudulentos en correos de phishing.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2024-923
Asunto	KIMSUKY REFUERZA SU CIBERATAQUE CON NUEVOS MALWARES
Emisión	26/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Un grupo de amenazas vinculado a Corea del Norte ha sido observado utilizando dos nuevas cepas de malware conocidas como KLogEXE y FPSpy. Esta actividad se atribuye a un adversario identificado como Kimsuky, que también es conocido bajo varias designaciones, incluyendo APT43, ARCHIPELAGO, Black Banshee, Emerald Sleet (anteriormente Thallium), Sparkling Pisces, Springtail y Velvet Chollima. Según los investigadores, estas nuevas muestras amplían el ya extenso arsenal de Sparkling Pisces, demostrando la continua evolución y creciente capacidad del grupo.

Kimsuky ha estado activo desde al menos 2012 y ha sido apodado el "rey del spear phishing" debido a su habilidad para engañar a las víctimas para que descarguen malware mediante correos electrónicos que aparentan ser de partes confiables. La investigación de los investigadores ha revelado la existencia de los ejecutables portátiles KLogEXE y FPSpy, que poseen capacidades para recolectar y exfiltrar información sobre las aplicaciones en ejecución en la estación de trabajo comprometida, así como las pulsaciones de teclas y clics del mouse.

KLogEXE es una versión en C++ de un keylogger basado en PowerShell llamado InfoKey, que fue destacado por JPCERT/CC en relación con una campaña de Kimsuky dirigida a organizaciones japonesas. Por otro lado, FPSpy es considerado una variante de un backdoor que se divulgó en 2022, y presenta similitudes con un malware bajo el nombre KGH_SPY a finales de 2020.

Además de la funcionalidad de keylogging, FPSpy está diseñado para recopilar información del sistema, descargar y ejecutar más cargas útiles, ejecutar comandos arbitrarios y enumerar unidades, carpetas y archivos en el dispositivo infectado. Los investigadores también identificaron similitudes en el código fuente de KLogEXE y FPSpy, lo que sugiere que probablemente fueron desarrollados por el mismo autor. La mayoría de los objetivos observados durante la investigación provenían de Corea del Sur y Japón, lo que es consistente con los patrones de ataque anteriores de Kimsuky.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-927
Asunto	STORM-0501 ATACA ENTORNOS DE NUBE CON EL DESPLIEGUE DE RANSOMWARE EMBARGO
Emisión	27/09/2024
CVE	No
Categoría	Ransomware
Severidad	CRÍTICA

Servicios Afectados

• Sistemas operativos Windows

Descripción

Storm-0501, un grupo de ciberamenazas que inicialmente surgió en 2021 como afiliado de la operación de Ransomware Sabbath, ha cambiado recientemente sus tácticas y ahora ataca entornos de nube híbridos, con el objetivo de comprometer todos los activos de las víctimas. Este grupo ha utilizado diferentes tipos de Ransomware como Hive, BlackCat, LockBit y Hunters International, y últimamente ha sido observado desplegando el Ransomware Embargo.

Los recientes ataques de Storm-0501 han tenido como objetivo hospitales, gobiernos, organizaciones manufactureras y de transporte, así como agencias de aplicación de la ley en Estados Unidos. El grupo de amenazas logra acceso a los entornos de la nube explotando credenciales débiles y abusando de cuentas privilegiadas, con el propósito de robar datos y ejecutar un Ransomware. Para acceder a las redes, Storm-0501 utiliza credenciales robadas o compradas, o bien aprovecha vulnerabilidades conocidas. Entre las fallas explotadas en ataques recientes se encuentran CVE-2022-47966 (Zoho ManageEngine), CVE-2023-4966 (Citrix NetScaler) y posiblemente CVE-2023-29300 o CVE-2023-38203 (ColdFusion 2016).

Una vez dentro de la red, el grupo se desplaza lateralmente utilizando marcos como Impacket y Cobalt Strike, y roba datos mediante un binario personalizado de Rclone, que renombraron para imitar una herramienta de Windows. Además, desactivan agentes de seguridad mediante comandos de PowerShell. Al obtener credenciales robadas de Microsoft Entra ID (anteriormente Azure AD), logran moverse de entornos locales a la nube, comprometiendo cuentas de sincronización y secuestrando sesiones para mantener la persistencia.

Las cuentas de Microsoft Entra Connect Sync son cruciales para sincronizar datos entre Active Directory locales y Microsoft Entra ID en la nube. Si los atacantes tienen las credenciales de estas cuentas, pueden usar herramientas como AADInternals para cambiar contraseñas en la nube, eludiendo protecciones adicionales. Si una cuenta de administrador de dominio o de alto privilegio también existe en el entorno en la nube y carece de protecciones adecuadas (como autenticación multifactor), los atacantes pueden usar esas mismas credenciales para acceder nuevamente a la nube.

Después de acceder a la infraestructura en la nube, los atacantes instalan un backdoor persistente creando un nuevo dominio federado dentro del inquilino de Microsoft Entra, lo que les permite autenticarse como cualquier usuario cuyo valor de "Immutableid" sea conocido o establecido por ellos. Finalmente, el grupo despliega el Ransomware Embargo tanto en los entornos locales como en la nube de la víctima, o bien mantiene acceso a la red para futuros ataques.

El Ransomware Embargo es parte de una operación de Ransomware como servicio (RaaS) que utiliza malware basado en Rust. Este modelo acepta afiliados que se encargan de vulnerar las redes de las víctimas para desplegar el Ransomware, compartiendo parte de las ganancias con los desarrolladores del malware. Microsoft ha observado que, en algunos casos, Storm-0501 no siempre recurre a la distribución del Ransomware, sino que se limita a mantener el acceso a la red mediante backdoor.

Actualización o Mitigación

• Implementar autenticación robusta, como autenticación de dos factores o autenticación basada en tokens, en lugar de depender únicamente de credenciales de usuario y contraseñas.

• Dividir la red en subredes puede limitar la propagación del Ransomware al controlar el tráfico entre ellas y restringir el movimiento lateral de los adversarios.

• Auditar las cuentas y configurar controles de acceso basados en el principio de privilegio mínimo puede reducir el riesgo de compromiso.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-931
Asunto	MALWARE MICROSOFT BLOCKED AFECTA A USUARIOS DE WINDOWS 10
Emisión	28/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows 10

Descripción

Un nuevo malware denominado "Microsoft Blocked" está causando estragos entre los usuarios de Windows 10 al reemplazar sus cuentas originales por una ficticia, lo que impide el acceso a sus dispositivos.

Al encender el ordenador, los afectados se encuentran con una pantalla de inicio de Windows alterada, donde su cuenta ha sido sustituida por "Microsoft Blocked". Al ingresar con la contraseña o PIN, no funciona.

Este ataque suele originarse al hacer clic en enlaces maliciosos o descargar archivos infectados, a menudo relacionados con software pirata.

Los ciberdelincuentes detrás de este malware no solo bloquean el acceso al sistema, sino que también exigen un rescate en criptomonedas a cambio de proporcionar la contraseña para la cuenta hackeada.

Actualización o Mitigación

• Utilizar autenticación de dos factores en la cuenta de Windows.

• Revisar y actualizar periódicamente las políticas de seguridad.

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-932
Asunto	LA NUEVA VARIANTE DE ROMCOM UTILIZADA EN ATAQUES DIRIGIDOS A MÚLTIPLES SECTORES
Emisión	28/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

SnipBot es una nueva variante del malware RomCom, descubierta por investigadores. Este malware ha sido utilizado en ataques que se centran en moverse lateralmente por la red comprometida para robar datos. Los investigadores analizaron un módulo DLL usado en los ataques de SnipBot y concluyeron que esta versión es una evolución significativa del malware RomCom, conocido previamente por ser utilizado en campañas de malvertising y phishing, así como para distribuir el Ransomware Cuba.

Las últimas campañas de SnipBot parecen estar dirigidas a una variedad de víctimas en diferentes sectores, incluidos los servicios de TI, el sector legal y la agricultura.

RomCom 4.0, la versión anterior del malware, ya contaba con capacidades como la ejecución de comandos, el robo de archivos, la modificación del registro de Windows y el uso de TLS para comunicaciones con el servidor de comando y control (C2). Sin embargo, SnipBot, considerado por los expertos como RomCom 5.0, ha extendido su conjunto de comandos a 27, permitiendo un control más preciso sobre las operaciones de exfiltración de datos. Esta nueva versión permite especificar tipos de archivos o directorios a ser robados, comprimir los datos usando la herramienta 7-Zip y extraer archivos comprimidos para evadir detección.

SnipBot también incorpora nuevas técnicas de ofuscación del flujo de control, dividiendo su código en bloques que son activados por mensajes personalizados de ventanas. Además, ha introducido métodos avanzados para evitar ser detectado en entornos de sandboxing, como realizar verificaciones de hash en el ejecutable y asegurar que existen al menos 100 entradas en los archivos "RecentDocs" y 50 subclaves en el registro "Shell Bags" de Windows.

El módulo principal de SnipBot, "single.dll", se almacena de manera cifrada en el Registro de Windows, desde donde se carga en la memoria para su ejecución. Otros módulos, como "keyprov.dll", también se descargan desde el servidor C2, se descifran y ejecutan en la memoria del sistema comprometido, lo que dificulta su detección.

En cuanto a los vectores de ataque, los investigadores rastrearon artefactos desde VirusTotal, descubriendo que las infecciones generalmente comienzan con correos electrónicos de phishing que contienen enlaces a archivos aparentemente inofensivos, como documentos PDF, diseñados para engañar a la víctima. También se identificó un vector anterior que involucraba un sitio web falso de Adobe, donde las víctimas eran engañadas para descargar una fuente faltante necesaria para ver un PDF, lo que activaba una cadena de redirecciones que terminaba en la descarga de un ejecutable malicioso.

El malware utiliza tácticas como el secuestro de objetos COM para inyectarse en procesos legítimos como "explorer.exe", lo que también le permite persistir en el sistema incluso después de un reinicio. Una vez comprometido el sistema, el actor malicioso recolecta información sobre la red de la empresa y el controlador de dominio, y roba archivos específicos de los directorios de Documentos, Descargas y OneDrive.

Después de la exfiltración inicial, se realiza una segunda fase de descubrimiento utilizando la utilidad AD Explorer, que permite ver y editar el Active Directory (AD). Los datos robados se archivan con WinRAR y se transfieren utilizando el cliente de copia segura PuTTY. Aunque los investigadores aún no tienen claro el objetivo final de estos ataques, sospechan que el actor malicioso ha cambiado su enfoque de obtener ganancias financieras a llevar a cabo operaciones de espionaje, dado el tipo de víctimas que han sido afectadas en las campañas recientes de SnipBot y RomCom.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2024-936
Asunto	NUEVA BOTNET GORILLABOT
Emisión	30/09/2024
CVE	No
Categoría	Malware
Severidad	ALTA

Servicios Afectados

• Sistemas operativos Windows

Descripción

La botnet, sería una versión modificada de Mirai, que es compatible con múltiples arquitecturas de CPU y emplea técnicas para mantener el control a largo plazo sobre los dispositivos infectados. Gorilla Botnet se dirige a sectores de infraestructuras críticas, como universidades, sitios web gubernamentales, telecomunicaciones y bancos.

La red de bots, cuyo objetivo eran diversas víctimas de 113 países, empleó principalmente ataques flood UDP. Paises como China, Estados Unidos, Canadá y Alemania se habrían llevado la mayor parte de los ataques, siendo especialmente vulnerables las organizaciones de infraestructuras críticas.

El malware GorillaBot, admite múltiples arquitecturas, utiliza un mensaje de firma para identificarse y se conecta aleatoriamente a uno de sus cinco servidores de C2 incorporados para recibir comandos.

A diferencia de su predecesor (Mirai), ofrece una gama más amplia de métodos de ataque DDoS, incluyendo UDP, TCP, GRE y ataques especializados dirigidos a protocolos específicos como OpenVPN, Discord y FiveM.

En un análisis se observó que GorillaBot emplea los algoritmos de cifrado usados por el grupo KekSec para salvaguardar las cadenas de datos críticos, mientras que la presencia de lol[.]sh en los scripts de propagación y en las firmas de código apunta a una posible conexión con KekSec.

Además, muestra una persistencia superior a la de los botnets Mirai típicos al aprovechar la función “yarn_init” para explotar una vulnerabilidad en Hadoop YARN RPC, lo que le permite obtener privilegios elevados.

Para garantizar su funcionamiento continuo, GorillaBot crea un archivo de servicio para el inicio automático e intenta descargar y ejecutar un script malicioso (lol[.]sh) desde varias ubicaciones al arrancar el sistema, al iniciar sesión el usuario o a través de scripts personalizados.

Es importante señalar que el bot identifica y evita los honeypots comprobando primero la presencia del sistema de archivos “/proc”.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

5. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, esto con la finalidad de encontrar más información de la amenaza como: Una mayor descripción, Indicadores de compromiso, recomendaciones personalizada y fuentes por amenaza.
- Considerar deshabilitar PowerShell y Macros de Microsoft, evitando que pueda ser aprovechado por softwares maliciosos.
- Utilizar una política de uso de contraseñas seguras considerando la complejidad, el cambio de credenciales por defecto y la no reutilización de las mismas.
- No almacenar credenciales en el Navegador Web, para que no sean obtenidos por malware stealer.
- Eliminar las cookies después de cada sesión del navegador para evitar el secuestro de datos.
- Contar con una solución EDR (Endpoint Detection and Response) para habilitar capacidades de detección y respuesta, como detener procesos y aislar sistemas de la red.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.
- Verificar la información de la cuenta que envía el correo, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear todo el software descargado de Internet antes de la ejecución.
- De detectar un correo spam, phishing o cualquier actividad anómala reportarlo. inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IoC's es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de sus servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

** Es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de los servicios, con el propósito de aplicar los cambios de manera controlada.