BOLETÍN INFORMATIVO N°194

AGOSTO 2025

Las fallas de CyberArk y HashiCorp permiten el acceso remoto a bóvedas sin credenciales

Los investigadores de ciberseguridad han descubierto más de una docena de vulnerabilidades en las bóvedas seguras empresariales de CyberArk y HashiCorp que, si se explotan con éxito, pueden permitir a atacantes remotos abrir los sistemas de identidad corporativa y extraer secretos y tokens empresariales de ellos.

El malware SocGholish se propaga mediante herramientas publicitarias y ofrece acceso a LockBit, Evil Corp y otros.

Se ha observado que los actores de amenazas detrás del malware SocGholish aprovechan los sistemas de distribución de tráfico (TDS) como Parrot TDS y Keitaro TDS para filtrar y redirigir a usuarios desprevenidos a contenido sospechoso.

Investigadores detectan un aumento en los exploits RCE de Erlang/OTP SSH; el 70 % ataca los firewalls OT.

Ya a principios de mayo de 2025 se ha observado que actores maliciosos explotan una falla de seguridad crítica, ahora parcheada, que afecta a Erlang/Open Telecom Platform (OTP) SSH, y aproximadamente el 70 % de las detecciones se originan en firewalls que protegen redes de tecnología operativa (OT).

RubyGems y PyPI afectados por paquetes maliciosos que roban credenciales y criptomonedas, forzando cambios de seguridad.

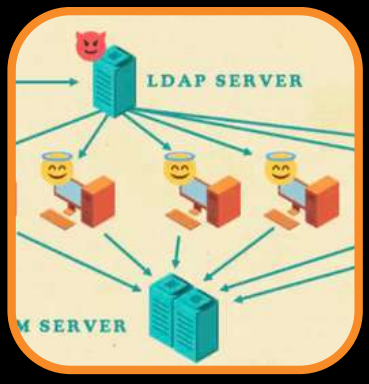
Se ha descubierto un nuevo conjunto de 60 paquetes maliciosos que apuntan al ecosistema RubyGems y se hacen pasar por herramientas de automatización aparentemente inocuas para redes sociales, blogs o servicios de mensajería para robar credenciales de usuarios desprevenidos y probablemente revenderlas en foros de la web oscura como Russian Market.

WinRAR Zero-Day bajo explotación activa: actualice a la última versión de inmediato

Los mantenedores de la utilidad de archivado de archivos WinRAR han publicado una actualización para abordar una vulnerabilidad de día cero explotada activamente.

RECOMENDACIONES

LECTURA DE SEGURIDAD



Win-DDoS: Los atacantes pueden convertir los controladores de dominio público en agentes DDoS

Los investigadores de SafeBreach han publicado detalles sobre varias vulnerabilidades que podrían ser explotadas por atacantes para bloquear los controladores de dominio (DCs) de Windows Active Directory, una de las cuales (CVE-2025-32724) también puede aprovecharse para obligar a los DCs públicos a participar en ataques distribuidos de denegación de servicio (DDoS).

Consejos de Windows para reducir la amenaza del ransomware

Dado que la identidad se está convirtiendo en una de las principales formas en que los atacantes obtienen acceso a las redes corporativas, los administradores de seguridad deben tomar el control de la autenticación de Windows y las políticas de acceso.

Resumen semanal: Ataque BadCam, WinRAR 0-Day, EDR Killer, fallas de NVIDIA, ataques de ransomware y más

Esta semana, los ciberatacantes se mueven con rapidez y las empresas deben mantenerse alerta. Están descubriendo nuevas debilidades en software popular y creando formas inteligentes de evadir la seguridad.

NOTICIAS DE

NUESTROS PARTNERS

Minimizar los permisos para la investigación forense en la nube: una guía práctica para reforzar el acceso en la nube

La mayoría de los entornos en la nube tienen dificultades para encontrar el equilibrio adecuado entre seguridad y accesibilidad. Este blog explica por qué los enfoques tradicionales de análisis forense en la nube suelen fallar y describe estrategias prácticas, priorizando la seguridad, para resolver el dilema del acceso.

Respuesta a incidentes mejorada basada en información sobre métricas de rendimiento

Resolver incidentes o encontrar las causas raíz es una actividad crucial que requiere evidencia registrada para comprender qué sucedió realmente en un sistema. Ya sea para evitar que estos incidentes se repitan o para descartar un intento de piratería maliciosa, obtener respuestas es fundamental, y los registros son la mejor fuente para obtener dicha evidencia.

Informe de IBM: El 13% de las organizaciones informaron sobre vulneraciones de modelos o aplicaciones de IA, y el 97% de ellas informaron carecer de controles de acceso de IA adecuados.

Informe sobre el Costo de una Filtración de Datos , que revela que la adopción de IA está superando ampliamente a la de su seguridad y gobernanza.

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE

NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información