Mainsoft®

BOLETÍN INFORMATIVO
#236 | Nov 2026

El archivo "Don't Ask Again" de Claude Code expone contraseñas y claves en 1122 copias públicas en GitHub.

Las contraseñas y las claves API que los desarrolladores introdujeron en los comandos que aprobaron en Claude Code se encuentran en repositorios públicos de GitHub, donde cualquiera puede leerlas.



ver artículo >>



OpenSSH emite una solución de emergencia para una vulnerabilidad que permitía que las contraseñas largas eludieran la autenticación SSH en Alpine Linux.

En algunos servidores Alpine Linux que ejecutan el paquete estándar openssh-server, los atacantes pueden iniciar sesión en cuentas sin contraseña, como las que solo utilizan claves SSH. Para ello, necesitan acceso a la red del servidor, un nombre de usuario y una contraseña de entre 257 y 1024 bytes.

ver artículo >>

Una vulnerabilidad APT en Debian y Ubuntu permite a atacantes MitM intercambiar paquetes verificados y ejecutar código como root.

Una vulnerabilidad en APT , el gestor de paquetes de Debian y Ubuntu, permite a un atacante que pueda modificar las descargas de paquetes sustituir un paquete verificado por uno propio.

ver artículo >>

Apple comenzará a escanear las fotos y archivos de iCloud compartidos públicamente en busca de contenido dañino.

Apple ha revelado que planea comenzar a revisar los enlaces públicos de iCloud en busca de contenido dañino a partir de iOS 27.3, iPadOS 27.3, macOS 27.3 y visionOS 27.3

ver artículo >>



INCIDENTES DE SISTEMAS



CISA advierte sobre una vulnerabilidad en SonicWall SonicOS SSLVPN que ha sido explotada en ataques.

CISA añadió una vulnerabilidad de SonicWall SonicOS SSLVPN, CVE-2026-19868, a su catálogo de vulnerabilidades explotadas conocidas , advirtiendo que los usuarios con credenciales válidas pueden eludir los controles de autenticación SAML y potencialmente evadir la autenticación multifactor.

ver artículo >>



Una vulnerabilidad crítica en los componentes del servidor de React permite a los hackers ejecutar código de forma remota sin autenticación.

Una vulnerabilidad de seguridad crítica en React Server Components permite a los atacantes ejecutar código de forma remota sin necesidad de iniciar sesión. React publicó el aviso, identificado como GHSA-xqc2-xf4c-x3h3, el 14 de octubre de 2026.

ver artículo >>



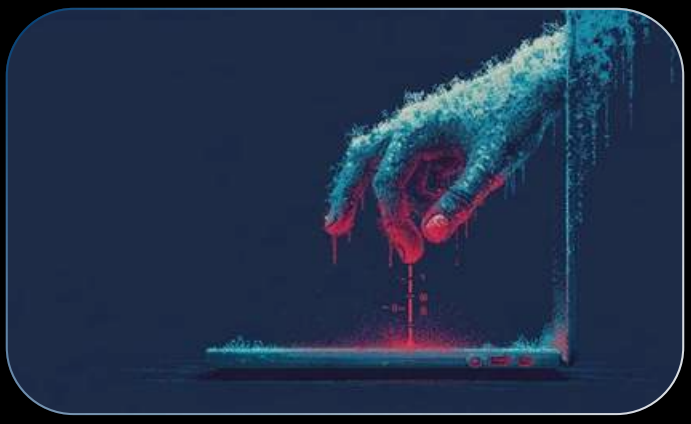
RECOMENDACIONES DE LECTURA DE SEGURIDAD

Resumen de la semana: Los ciberataques contra el sector de la refrigeración vuelven a afectar a los minoristas europeos, según las previsiones del Patch Tuesday.

Aquí les presentamos un resumen de algunas de las noticias, artículos, entrevistas y videos más interesantes de la semana pasada:

ver artículo >>





Los piratas informáticos abusan de los controladores de refrigeración para enviar spam y redirigir el tráfico proxy.

SecurityScorecard ha descubierto que los controladores de refrigeración conectados a Internet que se utilizan en supermercados e instalaciones de almacenamiento en frío están siendo pirateados y convertidos en infraestructura para una presunta red de bots de spam y servicios de proxy.

ver artículo >>



NOTICIAS DE NUESTROS PARTNERS



La preparación para la era post-cuántica comienza con la gobernanza del acceso privilegiado.

Los plazos federales obligan a las organizaciones a actualizar su ciberseguridad para la era post-cuántica. Sin embargo, no se pueden proteger los sistemas hasta que se sepa quién tiene acceso a ellos y cómo se conectan.

ver artículo >>



Dynatrace reconocida como líder en The Forrester Wave™: AIOps Platforms, Q4 2026.

Dynatrace fue reconocida como líder en The Forrester Wave™: AIOps Platforms, Q4 2026 , al recibir la puntuación más alta en la categoría de Oferta Actual y la puntuación más alta posible en 16 criterios.

ver artículo >>

El Laboratorio Nacional de Oak Ridge, IBM y AMD lanzan una nueva plataforma de codiseño para la corrección de errores cuánticos.

IBM, el Centro de Ciencias Cuánticas (QSC) financiado por el Departamento de Energía de EE. UU. en el Laboratorio Nacional de Oak Ridge (ORNL) y AMD (NASDAQ: AMD) presentaron hoy una nueva plataforma de codiseño para la corrección de errores cuánticos, que integra la computación cuántica y la computación de alto rendimiento.

ver artículo >>



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