Mainsoft®

BOLETÍN INFORMATIVO

#234 | Octubre 2026

PHP advierte de otro riesgo de ejecución remota de código sin parchear dos días después de los parches de emergencia para PHP2Shell.

PHP ha advertido sobre otra forma en que un atacante podría ejecutar código en un servidor web, dos días después de haber lanzado correcciones de emergencia para las fallas críticas de PHP2Shell.



ver artículo >>



Una vulnerabilidad en Microsoft Authenticator permite que aplicaciones de Android sin permisos roben tokens de cuentas de trabajo.

Microsoft ha corregido una vulnerabilidad en su aplicación Authenticator para Android que permitía que una aplicación maliciosa sin permisos se hiciera pasar por una aplicación de Microsoft de confianza, como Teams, y recopilara tokens de inicio de sesión para la cuenta de trabajo de la víctima.

ver artículo >>

La infraestructura expuesta revela cómo los afiliados de ransomware utilizaron agentes de IA para ejecutar intrusiones.

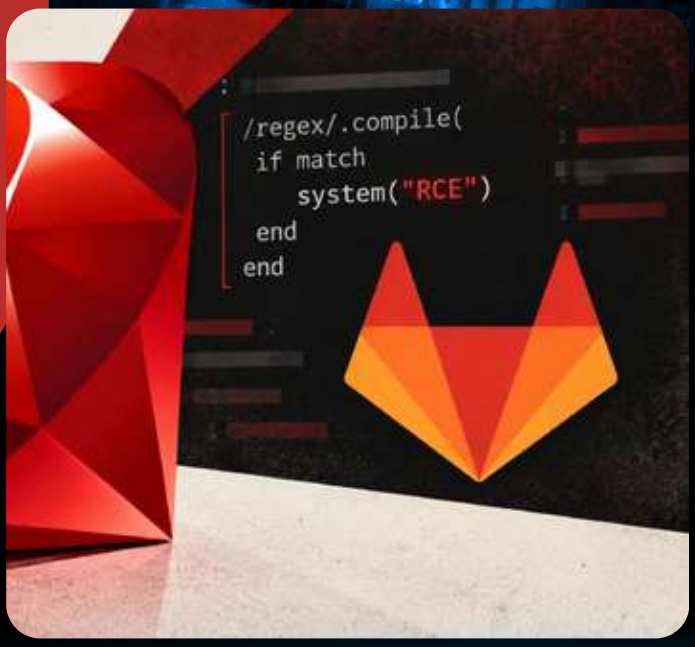
Investigadores de ciberseguridad han descubierto un ecosistema de intrusión impulsado por inteligencia artificial (IA) y gestionado por afiliados de los grupos de ransomware INC y The Gentlemen .



ver artículo >>



INCIDENTES DE SISTEMAS



Ruby corrige tres errores en su motor de expresiones regulares responsables de cuatro vulnerabilidades críticas de ejecución remota de código en GitLab.

Ruby ha lanzado las versiones 4.0.9, 3.4.12 y 3.3.13 para corregir tres errores en Onigmo, el motor de expresiones regulares integrado en el lenguaje. Estos errores son la causa de cuatro fallos de seguridad críticos que GitLab corrigió durante el último mes.

ver artículo >>



Apple lanza una actualización para corregir una vulnerabilidad de CoreGraphics en iPhones y iPads antiguos.

Apple implementó el lunes correcciones para una vulnerabilidad de seguridad grave que fue explotada en ciberataques reales en dispositivos más antiguos.

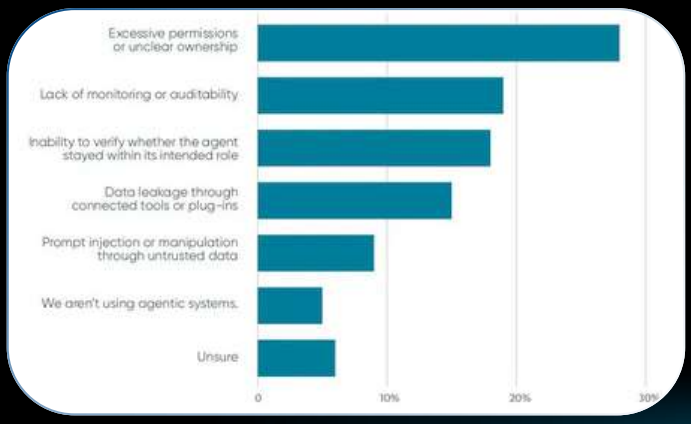
ver artículo >>



RECOMENDACIONES DE LECTURA DE SEGURIDAD

Los expertos en seguridad consideran que el mayor riesgo de la IA reside en la identificación de los empleados.

El hecho de que los empleados copien y peguen datos de la empresa en herramientas de IA preocupa más a los equipos de seguridad que los propios ataques impulsados por IA.



ver artículo >>



El 71% de la explotación de vulnerabilidades comienza dentro de la semana posterior a su divulgación.

Según el Informe Trimestral sobre el Panorama de Amenazas del tercer trimestre de 2026 de Rapid7, los atacantes explotan las vulnerabilidades de seguridad recién descubiertas en cuestión de días, lo que deja poco tiempo a las organizaciones para responder.

ver artículo >>

Resumen semanal: This2Shell, That2Shell, ¿Todo es un RCE? IA rebelde, caos en la cadena de suministro y más.

This2Shell, That2Shell, Everything2Shell. Así transcurrió la última semana. Están apareciendo por todas partes fallos críticos que permiten a los atacantes ejecutar código de forma remota.



ver artículo >>



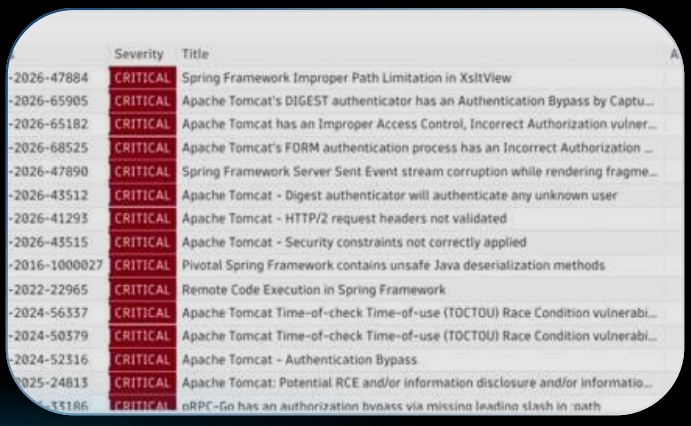
NOTICIAS DE NUESTROS PARTNERS



Vulnerabilidades de PHP, ARTEX y el creciente papel de la IA en los ciberataques

Las recientes revelaciones sobre PHP y las investigaciones publicadas sobre ARTEX indican que la IA se está utilizando en la investigación de vulnerabilidades y en operaciones ofensivas.

ver artículo >>



	Severity	Title
-2026-47884	CRITICAL	Spring Framework Improper Path Limitation in XsltView
-2026-65905	CRITICAL	Apache Tomcat's DIGEST authenticator has an Authentication Bypass by Captu...
-2026-65182	CRITICAL	Apache Tomcat has an Improper Access Control, Incorrect Authorization vulner...
-2026-68525	CRITICAL	Apache Tomcat's FORM authentication process has an Incorrect Authorization ...
-2026-47890	CRITICAL	Spring Framework Server Sent Event stream corruption while rendering fragme...
-2026-43512	CRITICAL	Apache Tomcat - Digest authenticator will authenticate any unknown user
-2026-41293	CRITICAL	Apache Tomcat - HTTP/2 request headers not validated
-2026-43515	CRITICAL	Apache Tomcat - Security constraints not correctly applied
-2016-1000027	CRITICAL	Pivotal Spring Framework contains unsafe Java deserialization methods
-2022-22965	CRITICAL	Remote Code Execution in Spring Framework
-2024-56337	CRITICAL	Apache Tomcat Time-of-check Time-of-use (TOCTOU) Race Condition vulnerabi...
-2024-50379	CRITICAL	Apache Tomcat Time-of-check Time-of-use (TOCTOU) Race Condition vulnerabi...
-2024-52316	CRITICAL	Apache Tomcat - Authentication Bypass
2025-24813	CRITICAL	Apache Tomcat: Potential RCE and/or information disclosure and/or informatio...
	CRITICAL	gRPC-Go has an authorization bypass via missing leading slash in :path

Exposición al riesgo de vulnerabilidad: vea la exposición en todos los procesos monitoreados en tiempo de ejecución.

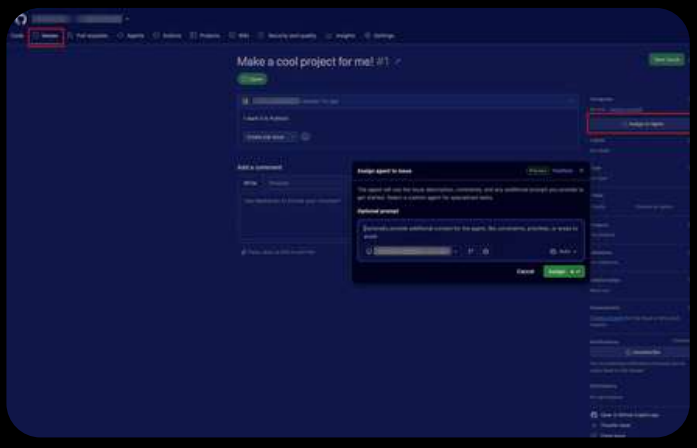
El nuevo panel de control de exposición al riesgo de vulnerabilidades de Dynatrace ofrece una visión consolidada de la exposición a vulnerabilidades en los hosts, procesos y entornos de Kubernetes monitorizados.

ver artículo >>

Cómo los comentarios ocultos en los problemas de GitHub pueden secuestrar a los agentes de Copilot

Qué tan seguras son las herramientas de codificación de IA frente a inyecciones ocultas de mensajes? En esta investigación, Phantom Labs demuestra cómo un comentario invisible en un problema de GitHub puede vulnerar el agente de codificación de GitHub Copilot, extraer información confidencial y escalar a CI/CD y la toma de control de la nube.

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