

SparroWocky: la amenaza silenciosa que se infiltra en organismos gubernamentales

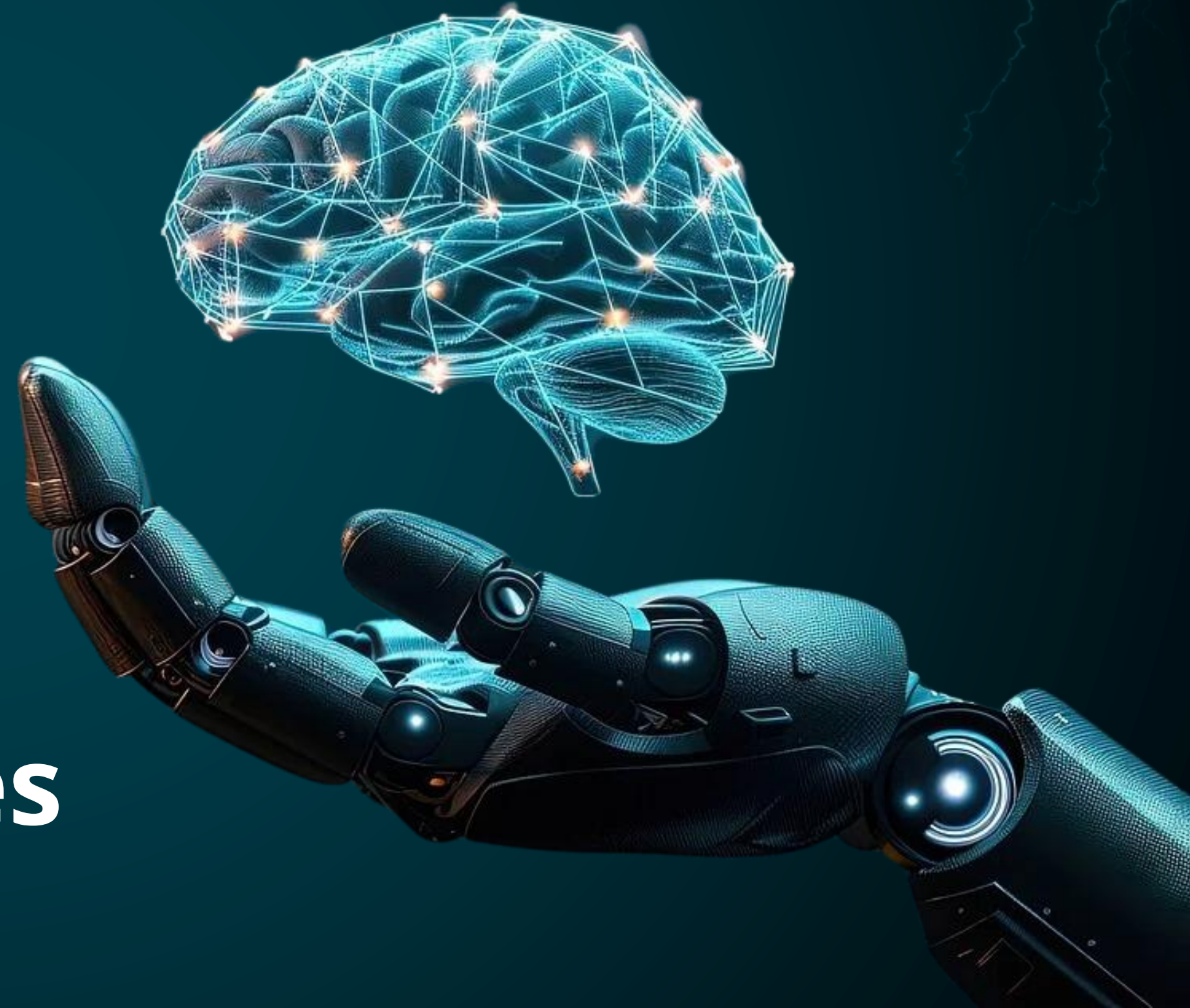
TLP:CLEAR
28.09.2026

CLICK PARA
EMPEZAR

CONTENIDO



-  **Nuestra Esencia**
-  **Vulnerabilidades**
-  **Noticias**
-  **Recomendaciones**



NUESTRA ESENCIA



BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.



EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.



SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.



Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CVE-2026-20079



Critical
(10.0)

Impacto: Ejecución arbitraria de comandos.

Resumen: Se identificó una vulnerabilidad crítica en Cisco Secure Firewall Management Center (FMC) que permite a un atacante remoto no autenticado eludir la autenticación y ejecutar scripts y comandos con privilegios root mediante solicitudes HTTP especialmente diseñadas.

Producto Afectado

- Cisco Secure Firewall Management Center (FMC) Software
- Cisco Security Cloud Control (SCC) Firewall Management.

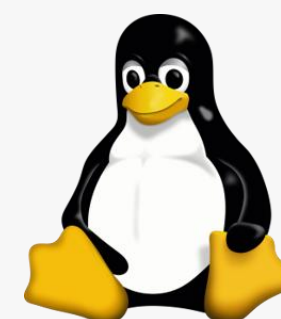
Ver +[INFO](#).

Solución:

Actualizar Cisco Secure FMC a una versión corregida

Ver + [INFO](#).

Fecha de Publicación: 16/SEP/2026  [+ INFO](#) 



KVM: arm64: Handle negative S1 walk levels in VNCR TLB size evaluation
CVE-2026-89775



Critical
(9.3)

Impacto: Corrupción o manejo incorrecto de la memoria virtual.

Resumen: Se identificó una vulnerabilidad en KVM del kernel de Linux para ARM64 relacionada con el cálculo incorrecto del tamaño de las invalidaciones de la TLB cuando la MMU S1 está deshabilitada. Esta condición puede provocar un tamaño de invalidación incorrecto durante la gestión de memoria virtual.

Producto Afectado

- Kernel de Linux con KVM para ARM64

Ver +[INFO](#).

Solución:

Actualizar a una versión del kernel que incluya la corrección de KVM

Ver +[INFO](#).

Fecha de Publicación: 16/SEP/2026  [+ INFO](#) 



Oracle Purchasing Unauthorized Data Access and Modification Vulnerability

CVE-2026-87168



High
(8.1)

Impacto: Acceso y modificación no autorizada de datos.

Resumen: Se identificó una vulnerabilidad fácilmente explotable en Oracle Purchasing de Oracle E-Business Suite que permite a un atacante con pocos privilegios y acceso de red mediante HTTP modificar, eliminar o acceder sin autorización a datos críticos.

Producto Afectado

- Oracle E-Business Suite 12.2.10 a 12.2.15

Ver +[INFO](#).

Solución:

Aplicar las actualizaciones de seguridad proporcionadas por Oracle para las versiones afectadas.

Ver +[INFO](#).

Fecha de Publicación: 22/SEP/2026



Adobe Commerce | Improper Neutralization of Special Elements Used in a Template Engine

CVE-2026-75650



Critical
(10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad en Adobe Commerce relacionada con la neutralización incorrecta de elementos especiales en un motor de plantillas, que podría permitir a un atacante ejecutar código arbitrario en el contexto del usuario actual sin requerir interacción del usuario.

Producto Afectado

- Adobe Commerce.

Ver +[INFO](#).

Solución:

Actualizar Adobe Commerce a una versión que incluya la corrección de seguridad.

Ver + [INFO](#).

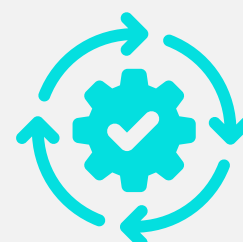
Fecha de Publicación: 09/SEP/2026





Oracle Critical Security Patch Update Advisory

CVE-2026-83348 – CVE-2026-83160
CVE-2026-83271 – CVE-2026-83272



Oracle lanzó su actualización crítica de seguridad de septiembre de 2026 con 673 parches que corrigen más de 800 vulnerabilidades, incluyendo más de 100 críticas y más de 240 explotables remotamente sin autenticación. Oracle E-Business Suite, Fusión Middleware e Hyperion concentraron gran parte de las correcciones. Oracle recomienda aplicar los parches lo antes posible.

Recomendación:

- Aplicar oportunamente las actualizaciones de seguridad de Oracle correspondientes a septiembre de 2026.

Productos Afectados

Algunos de los productos afectados son:

- Oracle E-Business Suite
- Fusion Middleware
- Hyperion

Ver [+INFO](#)

Fecha de Publicación: 16/SEP/2026



Google chrome releases

CVE-2026-91726 – CVE-2026-91721
CVE-2026-91749 – CVE-2026-91724



Google lanzó una actualización de seguridad para Chrome 153 que corrige 42 vulnerabilidades, incluidas 3 críticas y varias de alta gravedad. Los fallos afectan componentes como WebGL, Workers e Internals y podrían permitir ejecución de código o acceso no autorizado a datos. La actualización está disponible para Windows, macOS y Linux.

Recomendación:

- Actualizar Google Chrome a la versión más reciente disponible.

Productos Afectados:

Los productos afectados son:

- Google Chrome para Windows
- Google Chrome para MacOS
- Google Chrome para Linux

Ver [+INFO](#)

Fecha de Publicación: 16/SEP/2026



LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
16/09/2026	CVE-2026-20176	Cisco	9.9	Se identificaron vulnerabilidades en Cisco ISE que podrían permitir a un atacante autenticado ejecutar comandos arbitrarios en el sistema operativo. Cisco publicó actualizaciones de seguridad para corregirlas.
16/09/2026	CVE-2026-76423	Cisco	10.0	Se identificaron múltiples vulnerabilidades en Cisco ISE e ISE-PIC que podrían permitir eludir la autenticación, ejecutar código remotamente y realizar ataques de inyección SQL y XML. Cisco publicó actualizaciones para corregirlas.
16/09/2026	CVE-2026-20282	Cisco	9.1	Se identificaron múltiples vulnerabilidades en Cisco ISE que podrían permitir a un atacante autenticado realizar inyección SQL, modificar datos y ejecutar comandos arbitrarios. Cisco publicó actualizaciones de seguridad para corregirlas.
16/09/2026	CVE-2026-20305	Cisco	9.1	Se identificaron múltiples vulnerabilidades en Cisco ISE e ISE-PIC que podrían permitir a un atacante autenticado ejecutar comandos arbitrarios con privilegios root. Cisco publicó actualizaciones de seguridad para corregirlas.
21/09/2026	CVE-2026-87124	Oracle	7.7	Se identificó una vulnerabilidad en Oracle iRecruitment que podría permitir a un atacante con pocos privilegios y acceso mediante HTTP obtener acceso no autorizado a datos críticos. La explotación no requiere interacción del usuario.

SparroWocky: la amenaza silenciosa que se infiltra en organismos gubernamentales

ESET identificó una nueva campaña de ciberespionaje de FamousSparrow, grupo alineado con China, dirigida principalmente contra organismos gubernamentales de América Latina mediante la puerta trasera SparroWocky. El malware permite recopilar información del sistema, ejecutar comandos, realizar capturas de pantalla, exfiltrar archivos y establecer comunicaciones mediante proxy TCP, además de utilizar técnicas de evasión y persistencia.

Según ESET, cerca del 90 % de los objetivos identificados entre mediados de 2025 y 2026 se ubicaron en América Latina, con víctimas en Argentina, Ecuador, Guatemala, Honduras, Panamá, Perú, Puerto Rico y Venezuela. SparroWocky habría reemplazado al antiguo implante SparrowDoor.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver [+INFO](#).

EL ATAQUE

El ataque de FamousSparrow comienza mediante el despliegue de SparroWocky utilizando un esquema de carga lateral de DLL, donde un ejecutable legítimo carga una DLL modificada que recupera la carga útil cifrada.

El malware se carga de forma reflectiva en memoria para dificultar su detección y, una vez activo, recopila información del sistema, ejecuta comandos, realiza capturas de pantalla, exfiltra archivos y establece conexiones mediante proxy TCP.

Además, puede mantener la persistencia mediante servicios o claves de registro, permitiendo a los atacantes mantener el acceso al sistema comprometido y realizar actividades de espionaje dentro de las organizaciones afectadas.

CONTEXT	INDICATOR	(MD5)
SHA256	E0b6f8535e19f0a4938e3317de0c4493ecea17aa906fd0454805ba2086cbf3a8	922c1edb47fba94b548edca863165fb1
SHA1	Fdc44057e87d7c350e6df84bb72541236a770ba2	006f22e5e419d349e6459d0d5610105f
IPv4	103[.]85[.]25[.]166	N/A
IPv4	27[.]102[.]113[.]240	N/A
Dominio	amelicen[.]com	N/A
IPv4	130[.]94[.]101[.]82	N/A
IPv4	149[.]104[.]87[.]228	N/A
IPv4	149[.]104[.]90[.]203	N/A



+ INFO



ÚLTIMAS NOTICIAS

BragJack usa la IA del navegador contra el usuario

BragJack explota vulnerabilidades en la integración entre extensiones y agentes de IA de navegadores para secuestrar sus instrucciones y ejecutar acciones no autorizadas. El ataque afecta a Chrome con Gemini, Edge, Opera Neon, Perplexity Comet y Claude en Chrome, pudiendo permitir capturas de pantalla, acceso a archivos locales, cámara, micrófono y otra información sensible. Las vulnerabilidades ya fueron corregidas por los fabricantes, por lo que se recomienda mantener los navegadores actualizados y eliminar extensiones no autorizadas.

[+ INFO](#)

VectraRAT ataca Windows por \$250 al mes.

VectraRAT es una plataforma de Malware como Servicio (MaaS) que ofrece por 250 dólares al mes un implante para Windows, infraestructura C2 y panel de control, permitiendo a los ciberdelincuentes comprometer entornos empresariales. El malware puede distribuirse mediante Amadey Loader y campañas ClickFix, y proporciona acceso remoto, keylogging, robo de credenciales, transferencia de archivos y control de sistemas. Además, incorpora técnicas para evadir el UAC y recopilar automáticamente información sensible, facilitando el acceso persistente y posibles movimientos dentro de la red corporativa.

[+ INFO](#)

BambooToken controla sistemas mediante MQTT.

BambooToken es un malware multiplataforma que utiliza MQTT para controlar equipos Windows y Linux, recopilar información y ejecutar comandos. Ha sido detectado en organizaciones de Asia y Sudamérica, principalmente en sectores financieros, tecnológicos y gubernamentales. Además, puede cargar plugins, identificar las soluciones antivirus instaladas y mantener comunicaciones con servidores de mando y control mediante infraestructura oculta. Los investigadores han observado indicios de una posible conexión con China y señalan que su uso de MQTT permite gestionar múltiples equipos comprometidos de forma centralizada y discreta.

[+ INFO](#)

Una sola llave no debería abrir todas tus puertas

En ciberseguridad, incluso una contraseña compleja puede convertirse en un riesgo cuando se reutiliza en diferentes plataformas. Si una de esas cuentas es comprometida y la contraseña queda expuesta, los atacantes pueden intentar utilizarla para acceder a otros servicios.

- 🔑 Utiliza una contraseña diferente para cada cuenta y servicio.
- 🛡️ Activa la autenticación multifactor (MFA) siempre que esté disponible.
- 🔍 Revisa periódicamente tus cuentas y cambia las credenciales que puedan haber sido expuestas.
- 📋 Utiliza un gestor de contraseñas para generar y almacenar credenciales únicas y robustas.
- 🚨 Nunca compartas tus contraseñas ni las almacenes en lugares que no sean seguros.

Contraseñas únicas, cuentas más protegidas. Una sola filtración no debería abrir la puerta a todo lo demás.





DataSec



CYBERSOCDTS



csirt_datasec@datasec.com.co



+57 310 315 9346 Ext. 4



© 2025 DataSec SAS. Todos los Derechos Reservados
CYBERSOCDTS by DataSec