CIBER E-DEA

Boletín de Seguridad

Nueva brecha en Amazon ECS pone en riesgo la seguridad de contenedores

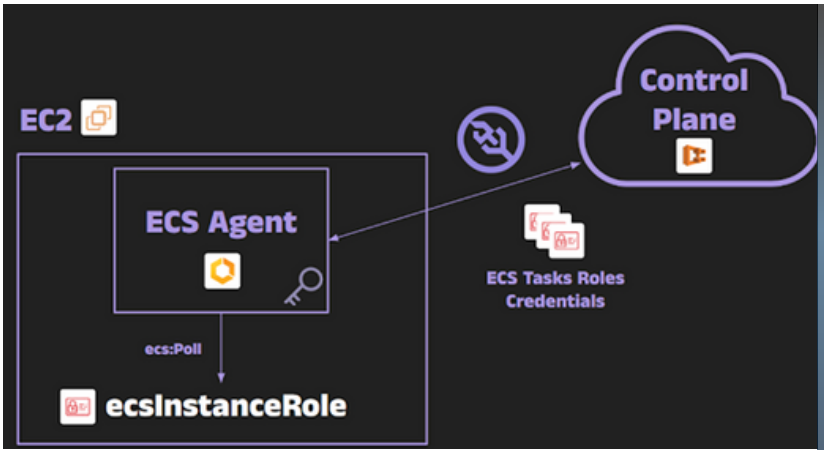
28.000 Servidores Exchange siguen sin parchearse

Ingenieria Social: El caso Cisco y la lección del vishing corporativo

WinRAR Zero-Day en explotación activa: actualice la ultima versión de inmediato

Ciber Incidentes en Colombia y en el Mundo

Nueva brecha en Amazon ECS pone en riesgo la seguridad de contenedores



Investigadores de **Sweet Security** descubrieron una falla crítica en Amazon ECS, llamada **ECScape**, que permite a contenedores con bajos privilegios acceder a credenciales de otros contenedores en la misma instancia EC2, rompiendo el aislamiento esperado entre tareas.

Presentado en **Black Hat USA 2025**, el ataque se basa en suplantar al agente ECS mediante un protocolo interno no documentado. El contenedor malicioso establece una conexión WebSocket falsa y recopila credenciales IAM de todas las tareas activas, imitando el comportamiento legítimo del sistema para evitar ser detectado.

Este tipo de ataque representa un riesgo serio en entornos compartidos, donde la falta de aislamiento puede facilitar el acceso no autorizado a datos sensibles y escalar privilegios dentro de la infraestructura cloud.

Secuencia del ataque ECScape:

- Obtiene credenciales del rol IAM de la instancia EC2.
- Descubre el punto final del plano de control de ECS.
- Reúne identificadores clave para autenticarse como agente.
- Falsifica la solicitud WebSocket con sendCredentials=true.
- Recopila credenciales de todas las tareas en ejecución.

Recomendaciones:

- Separar tareas críticas de tareas no confiables.
- Usar AWS Fargate para aislamiento real.
- Restringir el acceso al servicio de metadatos (IMDS).
- Limitar permisos del agente ECS.
- Configurar alertas en CloudTrail para detectar uso inusual de roles IAM.

Más información

Ingeniería social: El caso Cisco y la lección del vishing corporativo

El gigante tecnológico Cisco Systems confirmó un incidente de ciberseguridad que expuso información de usuarios registrados en su portal Cisco.com. La brecha se originó a partir de un sofisticado ataque de phishing por voz (vishing), que permitió a un actor malicioso acceder a un sistema CRM alojado en la nube y extraer datos de registro.

Aunque no se comprometieron contraseñas ni información financiera, el caso refleja la efectividad de las tácticas de ingeniería social dirigidas a empleados y su potencial como vector inicial de intrusión. (nombres, organizaciones, direcciones, correos, teléfonos).
No se comprometieron contraseñas, información financiera ni sistemas internos.

Recomendaciones clave:

- Capacitar al personal para identificar y rechazar llamadas sospechosas.
- Confirmar cualquier solicitud sensible por un canal distinto al de origen.
- Usar autenticación multifactor (MFA) en sistemas críticos y externos.
- Limitar accesos bajo el principio de mínimo privilegio.
- Realizar simulaciones internas de *vishing* para medir la respuesta.

Lección aprendida:

La tecnología protege, pero **la primera línea de defensa sigue siendo el criterio y la preparación del usuario**.

Más información

28.000 servidores Exchange siguen sin parchearse

En abril de 2025, Microsoft publicó parches y guías para corregir la vulnerabilidad CVE-2025-53786 en Microsoft Exchange, que permite a atacantes escalar privilegios en entornos de nube conectados si obtienen acceso administrativo a servidores locales. La CISA emitió una directiva de emergencia, pero al 1 de agosto de 2025 más de 28.000 servidores siguen sin parchear, exponiendo a muchas organizaciones.

Riesgos clave

- Escalamiento de privilegios entre entornos locales y la nube.
- Compromiso potencial de Exchange y Active Directory.
- Explotación de relaciones de confianza y cuentas privilegiadas olvidadas.

Thomas Richards (Black Duck): Es una vulnerabilidad grave y difícil de detectar. Parchear no basta: se deben rotar tokens de confianza para una remediación completa.

James Maude (BeyondTrust): Los entornos híbridos tienen cuentas de servicio invisibles o identidades no humanas (NHI) con altos privilegios. Estas NHI pueden acceder a sistemas locales y en la nube, y son un objetivo clave.

JElad Luz (Oasis Security): Implementar gestión moderna de identidades y gobernanza sólida para NHI. Migrar a identidades nativas de la nube siempre que sea posible. Mantener higiene de identidades: eliminar las obsoletas, revisar accesos y aplicar el Principio de Mínimo Privilegio. Usar credenciales de corta duración y rotación automatizadaames Maude (BeyondTrust): Los entornos híbridos tienen cuentas de servicio invisibles o identidades no humanas (NHI) con altos privilegios. Estas NHI pueden acceder a sistemas locales y en la nube, y son un objetivo clave.

Detalle de la Vulnerabilidad según la NIST

Microsoft publica la vulnerabilidad CVE-2025-53786 para documentar una vulnerabilidad que se soluciona siguiendo los pasos documentados en el anuncio del 18 de abril.

Puntuación Base: 8.0 ALTO
Vector de CVSS 3.1: AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

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

WinRAR, uno de los compresores más utilizados en Windows, ha corregido una vulnerabilidad grave ya explotada en la naturaleza y rastreada como CVE-2025-8088. El fallo, descubierto por los investigadores de ESET Anton Cherepanov, es un traversal de rutas (CWE-35) que permite a un archivo malicioso manipular la ruta de extracción y escribir ficheros fuera del directorio elegido por el usuario, posibilitando la ejecución de código. La entrada de NVD atribuye a la vulnerabilidad una severidad CVSS4 de 8,4 (alta) y la documenta como "explotada en el mundo real".

RARLAB ha publicado WinRAR 7.13 (31 de julio de 2025) indicando de forma explícita que "otra vulnerabilidad de directory traversal, distinta a la de WinRAR 7.12, ha sido corregida". En sus notas de versión, el proveedor detalla que versiones anteriores de WinRAR (y los componentes RAR/UnRAR para Windows, incluida UnRAR.dll) "pueden ser engañadas para usar una ruta definida dentro de un archivo especialmente diseñado en lugar de la especificada por el usuario". El problema afecta a Windows; la actualización 7.13 mitiga el vector.

La explotación ha sido reportada por varios medios y se ha observado en campañas de phishing que distribuyen RomCom (grupo vinculado a Rusia en distintos informes). En estos ataques, al abrir o extraer el RAR señuelo se consigue escribir ficheros en rutas sensibles, p. ej., la carpeta Startup, logrando que se ejecuten en el siguiente inicio de sesión.

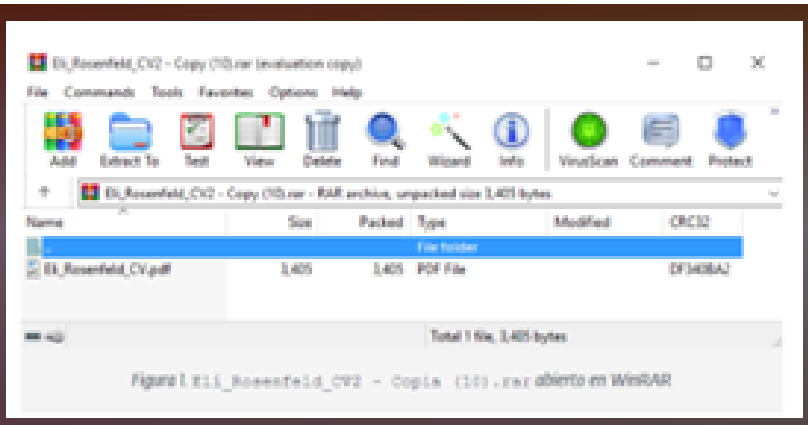


Figura 1. Eli_Rosenfeld_CV2 - Copia (10).rar abierto en WinRAR

Este 0-day llega poco después de CVE-2025-6218 (junio de 2025), otro directory traversal en WinRAR con impacto similar (escritura fuera del directorio y posible RCE) que también requería la interacción del usuario. El paralelismo entre ambos fallos subraya el atractivo de los gestores de archivos para los atacantes y la necesidad de actualizar con rapidez.

Recomendaciones

Actualiza de inmediato a WinRAR 7.13 y bloquea versiones anteriores. Endurece el manejo de adjuntos: filtra o aísla archivos .rar/.zip externos y, si es imprescindible abrirlos, hazlo en una sandbox. Supervisa escrituras a rutas sensibles (p. ej., Startup, AppData, ProgramData) realizadas por WinRAR.exe/UnRAR.dll y refuerza la concienciación: estos ataques suelen requerir interacción del usuario. Si tu entorno usa 7-Zip, actualiza también a la 25.01.

Vulnerabilidades destacadas

CVE-2025-25257

FortiWeb

Versiones afectadas
7.0.0 a 7.6.3

Es una vulnerabilidad que permite a los atacantes ejecutar comandos SQL dañinos sin iniciar sesión. Mediante el envío de solicitudes web especiales, pueden tomar el control total del sistema, incluso como root, instalar shells web, robar datos o comprometer completamente el dispositivo.

CVE-2025-6558

Google

Versiones afectadas
138.0.7204.157

Es una vulnerabilidad que permite a un atacante remoto eludir la zona protegida del navegador y potencialmente ejecutar código arbitrario aprovechando una validación de entrada insuficiente al procesar una página HTML especialmente diseñada

CVE-2025-20309

Cisco

Versiones afectadas
15.0.1.13010-1 a 15.0.1.13017-1

Es una vulnerabilidad que permitir que un atacante remoto no autenticado inicie sesión en un dispositivo afectado utilizando la cuenta raíz, que tiene credenciales estáticas predeterminadas que no se pueden modificar ni eliminar. Esta vulnerabilidad se debe a la presencia de credenciales de usuario estáticas para la cuenta raíz, reservadas para su uso durante el desarrollo.

Ciber incidentes en Colombia y en el mundo

Ciberseguridad en Colombia: Estrategias y Desafíos Actuales

Colombia enfrenta un panorama complejo en ciberseguridad debido al aumento de amenazas como ransomware, phishing y malware. En 2024, el país registró más de 36.000 millones de intentos de ciberataques, ubicándose entre los más afectados en América Latina.

El crecimiento de la transformación digital ha incrementado la exposición a riesgos, afectando tanto a ciudadanos como a empresas e instituciones. Aunque las denuncias de delitos informáticos bajaron un 10 % en 2023, siguen siendo elevadas, con Bogotá, Medellín y Cali como las ciudades más impactadas.

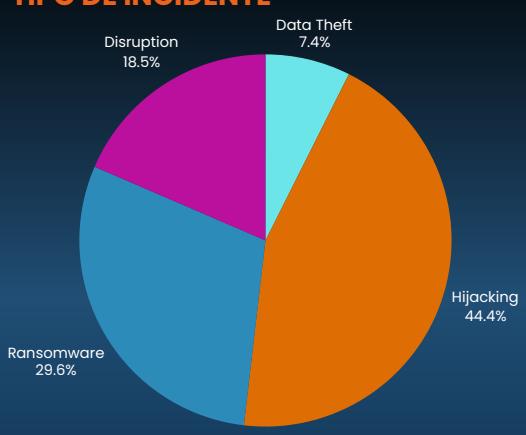
El gobierno impulsa políticas como el CONPES 3995 y la creación de la Agencia Nacional de Seguridad Digital, mientras que empresas y universidades incrementan inversiones y programas de formación en ciberseguridad. No obstante, persisten desafíos como la escasez de talento especializado, la sofisticación de los ataques con inteligencia artificial y la necesidad de fortalecer la cooperación público-privada.

Más información

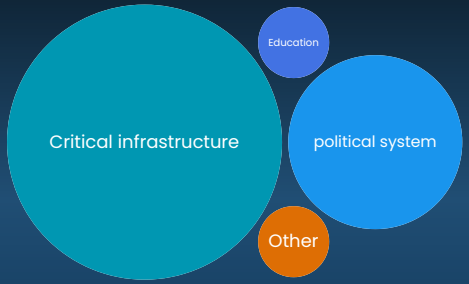
El mundo

27
Ciber incidentes

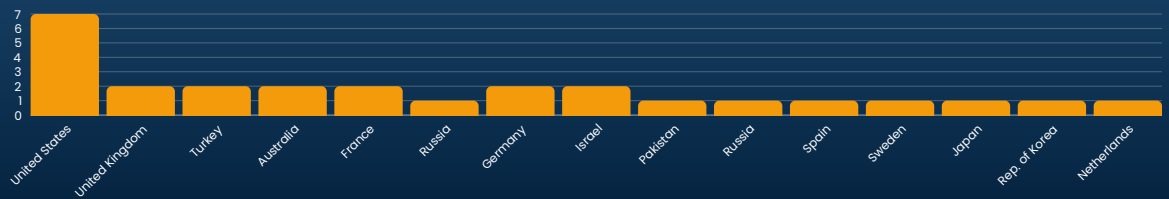
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co