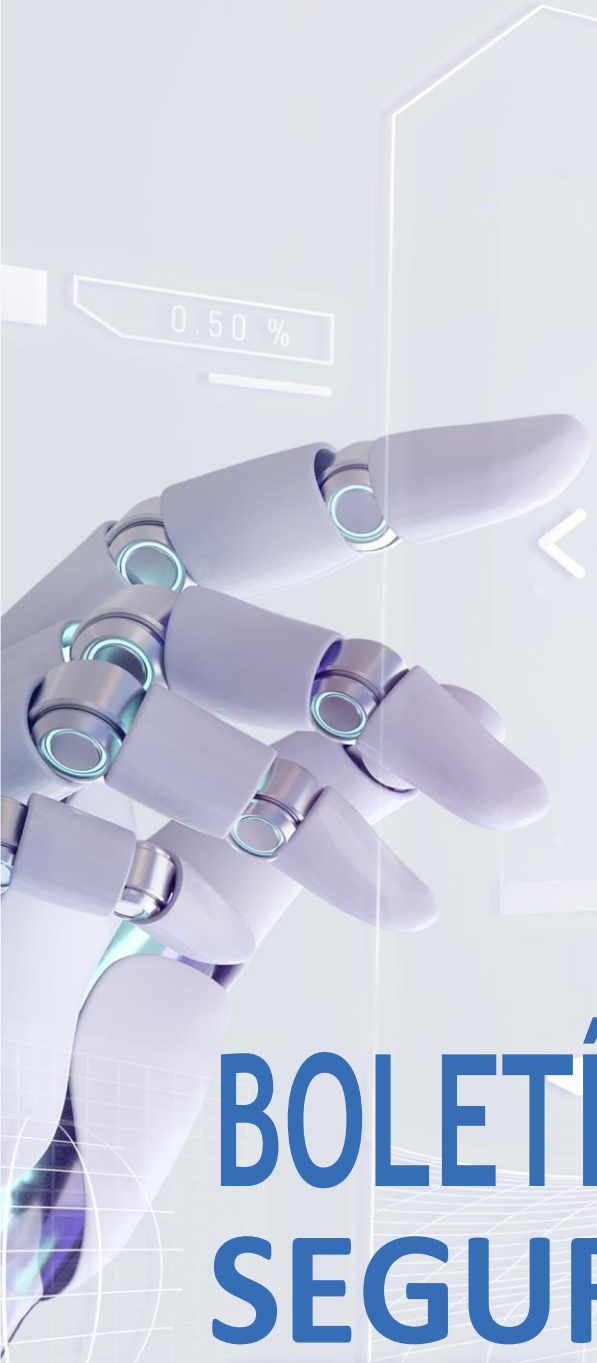
LUMA



BOLETÍN DE SEGURIDAD CIBERNÉTICA

28 de Marzo, 2025

TLP: CLEAR

Nueva Falla En VMware Tools Permite A Atacantes Elevar Privilegios En Máquinas Virtuales.

Impacto:
Alto - 7.8

CVE:
CVE-2025-22230

Descripción:

Una vulnerabilidad de omisión de autenticación en VMware Tools para Windows se informó de forma privada a VMware. Hay actualizaciones disponibles para remediar esta vulnerabilidad en los productos VMware afectados.

Recursos Afectados:

Busca afectar herramientas VMware Tools para Windows.

Solución:

Para remediar CVE-2025-22230, aplique los parches enumerados en la columna 'Versión fija' de la 'Matriz de respuesta' que se encuentra a continuación.

Matriz de Respuesta:

Producto VMware	Versión	Corriendo En	CVE	CVSSv3	Gravedad	Versión Fija
Herramientas VMware [2]	12.x.x, 11.x.x	Windows	CVE-2025-22230	7.8	Importante	12.5.1 [1]
Herramientas VMware	12.x.x, 11.x.x	Linux	CVE-2025-22230	N/A	N/A	No afectado
Herramientas VMware	12.x.x, 11.x.x	macOS	CVE-2025-22230	N/A	N/A	No afectado

[1] VMware Tools 12.4.6, que forma parte de VMware Tools 12.5.1, aborda el problema de Windows de 32 bits.
[2] Este problema solo afecta a VMware Tools para Windows.

Referencias:

- MISC:https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518
- URL:https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518

Vulnerabilidades críticas en Kubernetes permiten ejecución remota de código

Impacto:
Alto – 8.8

CVE:
CVE-2025-1097,
CVE-2025-1098,
CVE2025-24514,
CVE-2025-1974.

kubernetes

Descripción:
Investigadores de la empresa de seguridad en la nube Wiz han descubierto un conjunto de vulnerabilidades críticas en Ingress NGINX Controller para Kubernetes, denominadas IngressNightmare. Estas fallas, identificadas como CVE-2025-1097, CVE-2025-1098, CVE2025-24514 y CVE-2025-1974, permiten a atacantes remotos ejecutar código arbitrario y tomar control total de los clústeres de Kubernetes afectados. Dado que Ingress NGINX es ampliamente utilizado para exponer aplicaciones Kubernetes a internet, estas vulnerabilidades representan un riesgo severo para entornos empresariales y de infraestructura crítica.

Solución:
- Actualizar inmediatamente a las versiones parcheadas (1.12.1 o 1.11.5).
- Restringir el acceso al admission controller, asegurando que solo sea accesible desde el servidor API de Kubernetes.
- Deshabilitar temporalmente el admission controller si no es necesario para reducir la superficie de ataque.
- Consultar los avisos de seguridad de Kubernetes, Google Cloud y Microsoft para aplicar las mejores prácticas de mitigación.

Referencias:
- https://www.cve.org/CVERecord?id=CVE-2025-1097
- https://www.securityweek.com/ingressnightmare-flaws-expose-many-kubernetes-clusters-to-remote-hacking/

Chrome bajo ataque: Nueva vulnerabilidad zero-day explotada en campañas de phishing dirigidas

Impacto:
Alto – 8.3

CVE:
CVE-2025-2783

Descripción:
El manejo incorrecto proporcionado en circunstancias no especificadas en Mojo en Google Chrome en Windows en versiones anteriores a 134.0.6998.177 permitía a un atacante remoto realizar un escape SandBox a través de un archivo malicioso.

Recursos Afectados:
Primera vulnerabilidad zero-day de Chrome.

Solución:

- Actualizar Google Chrome y otros navegadores basados en Chromium (Edge, Brave, Opera, Vivaldi) a la versión más reciente.
- Asegurar que Chrome y otros navegadores se actualicen automáticamente para recibir parches de seguridad oportunos.
- Evitar hacer clic en enlaces sospechosos recibidos por correo, especialmente en contextos de foros académicos o gubernamentales.

Referencias:

- https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html
- https://issues.chromium.org/issues/405143032