e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

27 - julio – 2026

Vulnerabilidades en AWS

AWS publicó vulnerabilidades que afectan a sus productos.

Estás vulnerabilidades se encuentran asociadas a los CVE-2026-14904, CVE-2026-14471, CVE-2026-13763, CCVE-2026-13760, CVE-2026-14265 y CVE-2026-13762 que, en caso de ser explotadas, podrían: permitir a un atacante omitir reglas administradas por AWS WAF, Resolución incorrecta de enlace, Inyección de código SQL autenticada, Deserialización de datos no confiables e Inyección de comandos del sistema operativo.

Productos **afectados**

CVE	Producto	Versión afectada
CVE-2026-14904	AWS Research and Engineering Studio	<=2026.03
CVE-2026-14471	Servicios de metricas de mcp-gateway-registry	>=1.0.3 Y <=1.0.12
CVE-2026-14265	AWS Advanced JDBC Wrapper	>=3.3.0 Y <=4.0.0
CVE-2026-13760	AWS CDK (aws-cdk-lib)	< 2.260.0
CVE-2026-13763	AWS Web Application Firewall	NO ESPECIFICA
CVE-2026-13762	AWS Web Application Firewall	NO ESPECIFICA

Recomendaciones



Severidad: **Alta**

Parches

Actualizar a las versiones corregidas indicadas por el fabricante y validar la documentación.

Configuración

- *Habilitar la configuración del grupo de destino "Inspeccionar después de datos suficientes" asociada a un balanceador de carga ALB.*
- *Asegurarse de que cualquier código bifurcado o derivado haya sido actualizado para incorporar las nuevas revisiones.*

Fuentes: AWS SECURITY BULLETINS,