e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

10 - septiembre - 2026

Vulnerabilidad en PAN-OS

Un atacante sin autenticación y con acceso de red a la interfaz web de administración o de datos puede causar denegación de servicio en VM-Series o ejecutar código como root en PA-Series. Panorama también está afectado.

Productos afectados: PAN-OS

Producto	Versión afectada	Versión corregida
PAN-OS 12.2	< 12.2.3	12.2.3
PAN-OS 12.1	< 12.1.4-h10 < 12.1.7-h5 < 12.1.10	12.1.4-h10 12.1.7-h5 12.1.10
PAN-OS 11.2	< 11.2.4-h21 < 11.2.7-h20 < 11.2.10-h14 < 11.2.13-h2	11.2.4-h21 11.2.7-h20 11.2.10-h14 11.2.13-h2

Productos afectados: PAN-OS

Producto	Versión afectada	Versión corregida
PAN-OS 11.1	< 11.1.4-h36 < 11.1.6-h38 < 11.1.7-h10 < 11.1.10-h33 < 11.1.13-h12 < 11.1.16-h2	11.1.4-h36 11.1.6-h38 11.1.7-h10 11.1.10-h33 11.1.13-h12 11.1.16-h2
PAN-OS 10.2	< 10.2.7-h37 < 10.2.10-h40 < 10.2.13-h24 < 10.2.16-h10 < 10.2.18-h10	10.2.7-h37 10.2.10-h40 10.2.13-h24 10.2.16-h10 10.2.18-h10

Producto	Versión afectada	Versión corregida
Cloud NGFW	Todas en AWS y Azure	Ninguna en AWS o Azure
Prisma Access 12.1	< 12.1.7-h5	12.1.7-h5
Prisma Access 11.2	< 11.2.7-h20	11.2.7-h20
Prisma Access 10.2	< 10.2.10-h40	10.2.10-h40

Recomendaciones



Severidad: **Alta**

Parches

Actualizar a las versiones corregidas de las tablas, según la rama instalada.

Configuración

- *Restringir la administración a IP internas confiables o a un servidor de salto.*

Fuente: Palo Alto Networks CVE-2026-0310