e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

10 - julio – 2026

Vulnerabilidades en Paloalto

Detalles

Las vulnerabilidades permiten que un atacante explote PAN-OS enviando tráfico o entradas manipuladas provocando fallos de memoria en el User-ID Terminal Server Agent (con posible impacto de DoS o ejecución de código), Denegación de servicio en el procesamiento de red hasta dejar el equipo en modo de mantenimiento y ejecución de código ejecutado en la CLI como usuario ROOT.

Productos **afectados**

Producto afectado	Versiones	CVE
PAN- OS	12.1 – 11.2 – 11.1 – 10.2	**CVE-2026-0286 - CVE-2026-0288 - CVE-2026-0287**
Prisma Access	11.2.0 -10.2.0	**CVE-2026-0288- CVE-2026-0287**
Cloud NGFW	Afectado en todos los despliegues de AWS y Azure	**CVE-2026-0287**

Severidad: **Alta**

Recomendaciones

Parches	Actualizar a las versiones corregidas indicadas por el fabricante y validar la documentación.
Configuración	Restringir la conectividad del Terminal Server Agent (TSA) a solo IPs internas confiables y verificar si el dispositivo tiene al menos una entrada de TSA configurada.
	Restringir el acceso a la CLI a un grupo reducido de administradores o usar Threat Prevention habilitando el Threat ID 510036 (requiere SSL Decryption).

Fuentes: Palo Alto Networks Security Advisories,