UNIDAD DE CIBERDEFENSA NAVAL

ALERTA DE SEGURIDAD INFORMÁTICA

Fecha de emisión: 20/02/2025 **ALERTA-FEB-2025-010**
Clasificación de la alerta: CRÍTICO
Sistema afectado: Palo Alto Networks PAN-OS
Tipo de amenaza: Bypass de autenticación
Área afectada: Interfaz web de administración de PAN-OS
Importancia: 9.0

CVE-2025-0108 es una vulnerabilidad crítica en el software PAN-OS de Palo Alto Networks, la cual permite que un atacante no autenticado, con acceso a la red donde se encuentra la interfaz web de administración, pueda omitir el proceso de autenticación y ejecutar ciertos scripts PHP. Si bien esta vulnerabilidad no permite la ejecución remota de código, sí puede comprometer la integridad y confidencialidad del sistema.

Impacto potencial:
La explotación de esta vulnerabilidad podría permitir:

- Acceso no autorizado a la administración del firewall PAN-OS.
- Modificación de configuraciones críticas.
- Exposición de información sensible del sistema.

Indicadores de Compromiso (IoCs):

- Registros de acceso con intentos no autenticados en la interfaz de administración.
- Cambios no autorizados en configuraciones de PAN-OS.
- Uso anómalo de scripts PHP en los registros del sistema.

Recomendaciones:

- Restringir acceso a la interfaz web de administración: Configurar reglas en el firewall para permitir el acceso solo desde direcciones IP internas y de confianza.
- Monitorear registros: Auditar los registros de acceso y actividad en la interfaz de administración para detectar intentos sospechosos.
- Aplicar las mejores prácticas recomendadas: Seguir las recomendaciones de seguridad de Palo Alto Networks disponibles en su página web.
- Actualizar PAN-OS: Aplicar parches o actualizaciones proporcionadas por Palo Alto Networks en cuanto estén disponibles.

Acciones recomendadas para usuarios:

1. Deshabilitar el acceso a la interfaz web de administración desde redes no confiables.
2. Habilitar autenticación multifactor (MFA) para mejorar la seguridad de acceso.
3. Capacitar al personal en seguridad de acceso y gestión segura de dispositivos PAN-OS.

Contacto para reportes:
Ante un incidente de seguridad informática se deberá reportar al correo csirt@armada.mil.ec, o mediante la página csirt.armada.mil.ec seleccionando en la opción del menú “Reportar Incidente”.

¡Reporta Aquí!