BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-31
Fecha de publicación: 11/09/2024
Tema: Vulnerabilidades Críticas en productos de Palo Alto Networks
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- PAN-OS (Sistema Operativo para Firewalls de Palo Alto Networks) versión 11.2.3 y anteriores.
- GlobalProtect (Solución de acceso remoto) en versiones anteriores a 6.2.1, 6.1.2 6.0.7, 5.2.13 y 5.1.12.
- Prisma Access y Prisma SD-WAN (Plataforma de seguridad en la nube y Solución de red de área extensa definida por software) no se han especificado versiones exactas.
- Cortex XDR (Plataforma de protección avanzada contra amenazas) no se han especificado versiones exactas.

Descripción

El equipo de Palo Alto Networks ha publicado vulnerabilidades críticas que afectan a los productos PAN-OS, GlobalProtect, Cortex XDR y Prisma Access. Como ser la CVE-2024-8686 con score 8.6 y CVE-2024-8687 con score 6.9.

A continuación, detallamos las vulnerabilidades criticas relevantes:

CVE-2024-8686: Afecta a PAN-OS y permite que un administrador autenticado ejecute comandos arbitrarios con privilegios de root, lo que podría llevar a la toma de control total del sistema. Un atacante que explote esta vulnerabilidad podría eludir las restricciones de seguridad del sistema y ejecutar cualquier comando, lo que pone en riesgo la integridad del firewall. Es necesario acceso administrativo autenticado, lo que limita los ataques a aquellos con credenciales válidas, pero el impacto es severo si se explota

CVE-2024-8687: Esta vulnerabilidad expone credenciales de GlobalProtect en texto claro, lo que permite a los usuarios acceder a las contraseñas de desinstalación o desconexión de GlobalProtect. Esto permite a un usuario eludir restricciones de seguridad configuradas

por el administrador, como la imposibilidad de desactivar GlobalProtect. Además, podría permitir que un atacante desinstale o deshabilite GlobalProtect, dejando la red o dispositivo sin la protección de VPN, lo que abre la puerta a accesos no autorizados y filtración de datos

Solución

Para solucionar las vulnerabilidades reportadas en los productos de Palo Alto Networks, es esencial actualizar PAN-OS a la versión 11.2.3, y GlobalProtect a las versiones más recientes como 6.2.1, 6.1.2, 6.0.7, 5.2.13, o 5.1.12. Además, se deben aplicar los parches correspondientes a Cortex XDR y Prisma Access.

Para descargar las versiones más recientes de **PAN-OS** y **GlobalProtect**, debes acceder al **Portal de Soporte** de Palo Alto Networks: https://sso.paloaltonetworks.com/

Información adicional:

- https://www.securityweek.com/palo-alto-networks-patches-dozens-of-vulnerabilities
- https://securityonline.info/pan-os-vulnerabilities-command-injection-cve-2024-8686-and-globalprotect-exposure-cve-2024-8687

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com