BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-09
Fecha de publicación: 12/04/2024
Tema: Vulnerabilidad activamente explotada en GlobalProtect de Palo Alto.
Traffic Light Protocol (TLP): White

Producto afectado:

- GlobalProtect Gateways con el siguiente software que tengan habilitada la función de telemetría de dispositivo.:

PAN-OS Menor que 11.1.2-h3
PAN-OS Menor que 11.0.4-h1
PAN-OS Menor que 10.2.9-h1

Descripción

Palo Alto advierte que una falla en el software PAN-OS utilizado en sus gateways GlobalProtect está siendo activamente explotada. Denominada la vulnerabilidad como “CVE-2024-3400”, cuenta con una puntuación de CVSS de 10, indicando máxima severidad.

Según el fabricante, si las condiciones para la explotabilidad de esta vulnerabilidad coinciden, esto puede dar a lugar que un atacante no autorizado pueda ejecutar código arbitrario con privilegios elevados en el dispositivo.

De acuerdo con algunos investigadores, esta vulnerabilidad parece estar siendo explotado por un grupo de origen chino que probablemente también estuvo involucrados en el desarrollo de los exploits de diferentes productos de Vmware, Ivanti, Fortinet y Barracuda Networks. En esa ocasión, los atacantesluego de realizar la explotación de los productos, instalaban un backdoor para tener persistencia en los dispositivos.

Palo Alto reporta que esta vulnerabilidad está siendo explotada activamente, aunque todavía se ha visto un número limitado de casos. Sin embargo, es posible que próximamente aumente la cantidad de intentos de explotación.

Al revisar en fuentes OSINT, específicamente en Shodan, podemos encontrar que existen más de 500 dispositivos expuestos en México, y en E.E.U.U. más de 17 mil que están relacionados los Gateway de Palo Alto.

Impacto

Por lo que compartió el fabricante, los atacantes, sin previa autorización, pueden llegar a ejecutar código arbitrario con privilegios de administrador en los dispositivos afectados.

Solución

El parche para el arreglo de esta vulnerabilidad aún está en desarrollo y se estima que estará disponible hasta el día 14 de abril del presente año.

El equipo Beacon Lab recomienda con insistencia llevar a cabo la mitigación y esperar a la publicación del parche.

Mitigación

Si contamos con una licencia de Threat Prevention, se puede habilitar la regla Threat Id 95187, además de aplicar la protección de vulnerabilidad a su interfaz de GlobhalProtect.

Un workaround, para evadir la explotación de la vulnerabilidad es deshabilitar la funcionalidad de telemetría del dispositivo:

(Device > Setup > Telemetry)

Información adicional:

- CVE-2024-3400: Critical Command Injection Vulnerability in Palo Alto Networks Firewalls | Rapid7 Blog
- Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400 (paloaltonetworks.com)
- Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400) | Volexity
- Zero-Day Alert: Critical Palo Alto Networks PAN-OS Flaw Under Active Attack (thehackernews.com)

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com