

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

VULNERABILIDAD ZERO-DAY EN FIREWALL PAN-OS DE PALO ALTO NETWORKS

12/04/2024

CONTENIDO

INTRODUCCIÓN	3
RESUMEN	5
NOTICIA COMPLETA	7
CONTACTOS DE SOPORTE	8

INTRODUCCIÓN

En un panorama cibernético cada vez más complejo, la reciente advertencia de Palo Alto Networks sobre una vulnerabilidad crítica en sus firewalls PAN-OS subraya la urgencia de la seguridad cibernética en el mundo empresarial. La amenaza representada por CVE-2024-3400, una vulnerabilidad de inyección de comandos activamente explotada, resalta la importancia de la preparación y la acción proactiva frente a las crecientes ciberamenazas. En este breve análisis, exploraremos la naturaleza de esta vulnerabilidad, su impacto potencial y las medidas que las empresas pueden tomar para proteger sus sistemas y datos en un entorno digital cada vez más peligroso.

VULNERABILIDAD ZERO-DAY EN FIREWALL PAN-OS DE PALO ALTO NETWORKS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_04_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	12/04/2024
Es día cero (0 day):	Sí

RESUMEN

En una alerta que ha sacudido al mundo de la ciberseguridad, Palo Alto Networks ha revelado la existencia de una vulnerabilidad de inyección de comandos no parcheada en su firewall PAN-OS, que está siendo activamente explotada en ataques.

La Amenaza Descubierta

La vulnerabilidad, detectada por Volexity y rastreada como CVE-2024-3400, es una brecha de inyección de comandos que ha recibido la máxima puntuación de gravedad, 10.0. Lo alarmante es que no requiere privilegios especiales ni interacción del usuario para ser explotada.

Impacto y Soluciones

La vulnerabilidad afecta a versiones específicas del software PAN-OS cuando tanto la puerta de enlace GlobalProtect como las características de telemetría del dispositivo están habilitadas. Las versiones vulnerables incluyen PAN-OS 10.2, 11.0 y 11.1. Afortunadamente, se esperan correcciones para estas versiones antes del 14 de abril de 2024.

Para abordar la amenaza inminente, Palo Alto Networks lanzará hotfixes con las siguientes versiones:

- PAN-OS 10.2.9-h1

- PAN-OS 11.0.4-h1

- PAN-OS 11.1.2-h3

Productos como Cloud NGFW, dispositivos Panorama y Prisma Access no se ven afectados por esta vulnerabilidad.

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.2-h3	>= 11.1.2-h3 (ETA: By 4/14)
PAN-OS 11.0	< 11.0.4-h1	>= 11.0.4-h1 (ETA: By 4/14)
PAN-OS 10.2	< 10.2.9-h1	>= 10.2.9-h1 (ETA: By 4/14)
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All


Medidas de Mitigación

Dado que CVE-2024-3400 ya está siendo explotado activamente, los usuarios afectados deben aplicar mitigaciones de inmediato para reducir el riesgo hasta que estén disponibles las actualizaciones de seguridad. Las medidas propuestas incluyen:

- Bloquear ataques activando 'Threat ID 95187' para usuarios con una suscripción activa de 'Prevención de Amenazas'.
- Configurar la protección de vulnerabilidades en las 'Interfaces de GlobalProtect' para prevenir la explotación.
- Deshabilitar la telemetría del dispositivo hasta que se apliquen los parches de corrección.

Consecuencias Potenciales



Según el investigador de amenazas Yutaka Sejiyama, hay aproximadamente 82,000 dispositivos expuestos en línea que podrían ser vulnerables a CVE-2024-3400, con un 40% ubicado en los Estados Unidos.

nekono_nanomotoni 
 @nekono_naha

palo aloto告されています。公開台数はWWで82k台、国内1.7k台有り海外4-3400 ⚠️

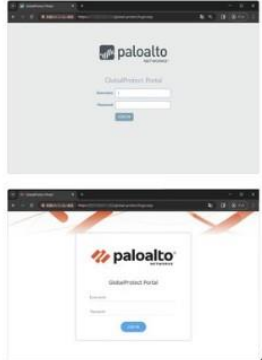
Traducido del japonés por Google

Se anunció una vulnerabilidad RCE de autenticación previa CVE-2024-3400 para una versión relativamente nueva de PAN-OS de Palo Alto, y ya se han informado vulnerabilidades. El número de servidores expuestos es 82.000 en WW, 1.7.000 en Japón y hay muchos servidores japoneses en el extranjero. Se recomienda a los usuarios que tomen medidas lo antes posible y estén atentos a la información más reciente ⚠️

¿Fue precisa esta traducción? Danos tu opinión para que podamos mejorar:  

Palo Alto: Global Protectを公開するサーバの台数
※2024年4月12日現在に13個国より取得したデータをもとに
※本表は公開されているサーバの台数を示す
※サーバ数ではなくユニークなIPアドレス数をカウントし、数値の多いTOP50を掲載

Country	Number	Country	Number
Global	82198	25 Hong Kong	561
1 United States	32916	26 Switzerland	561
2 Germany	3268	27 Colombia	527
3 United Kingdom	3213	28 Indonesia	521
4 India	2823	29 Finland	520
5 Australia	2423	30 UAE	479
6 Canada	2239	31 Austria	463
7 Singapore	2055	32 Denmark	445
8 France	1794	33 Korea	444
9 Italy	1759	34 Philippines	433
10 Japan	1721	35 Viet Nam	412
11 Ireland	1705	36 Saudi Arabia	387
12 China	1445	37 Peru	374
13 Netherlands	1370	38 Malaysia	362
14 Taiwan	1344	39 South Africa	306
15 Brazil	1166	40 Russian Federation	294
16 Portugal	1116	41 Chile	279
17 Poland	1065	42 Hungary	255
18 Mexico	922	43 Argentina	240
19 Spain	908	44 Israel	230
20 Thailand	907	45 Czech Republic	213
21 Turkey	830	46 New Zealand	211
22 Belgium	777	47 Slovenia	184
23 Sweden	651	48 Ecuador	185
24 Norway	640	49 Azerbaijan	177
		50 Egypt	175



3:25 a. m. · 12 de abril de 2024 · **8.874** Puntos de vista

Palo Alto Networks es consciente del riesgo inherente a sus dispositivos en redes corporativas, recordando un incidente anterior en agosto de 2022 cuando hackers aprovecharon otro zero-day en PAN-OS para llevar a cabo ataques de denegación de servicio amplificado (DoS) TCP.

Acción Urgente

Ante la gravedad de la situación, es crucial que los administradores tomen medidas inmediatas para asegurar sus sistemas. Con la amenaza latente, la seguridad cibernética se convierte en una prioridad ineludible para proteger los activos digitales y la continuidad del negocio.

NOTICIA COMPLETA

<https://devel.group/blog/vulnerabilidad-zero-day-en-firewall-pan-os-de-palo-alto-networks/>

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>