

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**Gitlab corrige vulnerabilidades en
una nueva actualización.**

8/julio/2022

Contenido

Introducción	3
Palo Alto	4
Resumen	4
Recomendaciones.....	6
Noticia Completa	6
Enlaces de Interes.....	6
Contactos de soporte	7

INTRODUCCIÓN

En este boletín, mostramos información brindada por Palo Alto sobre posibles fallos de navegación en sus versiones 9.1.13 y 10.0.10, se detalla el error y como solucionarlo por parte del fabricante.

PALO ALTO

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

ID de alerta:	DSOC-CERT_2022_07_08_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	MEDIO
TLP (Clasificación de información):	WHITE
Fecha de publicación:	07/08/2022
Es día cero (0 day):	NO

RESUMEN

Después de actualizar PAN-OS a 9.1.13 o 10.0.10, puede ocurrir una falla de tráfico inesperada y el registro de tráfico muestra el motivo de finalización de la sesión "recursos no disponibles".

Ambientes afectados:

Todas las plataformas, incluidos los cortafuegos de máquinas virtuales

Firewalls que se ejecutan en PAN-OS 9.1.13 (incluye h1 y h3) o 10.0.10 (no incluye h1)

Otras versiones de PAN-OS NO se ven afectadas por este problema

Causa:

Si puede ver el motivo de finalización de la sesión "recursos no disponibles" en el registro de tráfico sin pico de uso de recursos después de actualizar PAN-OS a las versiones afectadas, verifique si el contador "aho_alloc_lookup_failed" está aumentando o no.

```
> show counter global name aho_alloc_lookup_failed
```

```
Name:      aho_alloc_lookup_failed
```

```
Value:     184328 <<<<<-----!!!!!!
```

```
Severity:   Warning
```

```
Category:   aho
```

```
Aspect:     resource
```

```
Description: failed to alloc regex lookup
```

Si puede ver que el contador anterior está aumentando, verifique también si los "Resultados Regex" están agotados.

```
> debug dataplane pool statistics | match "Regex Results"
```

```
[12] Regex Results      (13272):  15/8192  0x8000000109219180
```

Si su firewall coincide con los síntomas anteriores, el problema podría estar afectando a PAN-189468.

Abra un nuevo caso de soporte a través de CSP con la carga del archivo de soporte técnico, si necesita nuestra ayuda para verificar la condición.

Resolución:

Este problema se solucionó en PAN-OS 9.1.14 y 10.0.10-h1. Actualice PAN-OS si está utilizando versiones afectadas (PAN-189468 solo afecta a 9.1.13, 9.1.13-h1, 9.1.13-h3 y 10.0.10).

Para liberar el grupo de memoria "Regex Result" en los PAN-OS afectados, debe reiniciar el firewall.

RECOMENDACIONES

- Se recomienda agendar una ventana de mantenimiento para poder aplicar las actualizaciones correspondientes y así evitar que el bug afecte el funcionamiento de su equipo.
- Realizar un backup de configuraciones antes y después de aplicar la actualización.

NOTICIA COMPLETA

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004ODICA2>

ENLACES DE INTERES

PAN-OS 9.1.14 Issues : <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes/pan-os-9-1-addressed-issues/pan-os-9-1-14-addressed-issues#panos-addressed-issues-9.1.14>

PAN-OS 10.0.10-h Issues: <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-release-notes/pan-os-10-0-addressed-issues/pan-os-10-0-10-h1-addressed-issues>

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>