swpanel

SEGURIDAD AVANZADA · NGFW

Informe de amenazas swpanel.com

Lo que el cortafuegos NGFW ha detectado y bloqueado en swpanel.com (203.0.113.10) del 13 de septiembre al 12 de octubre de 2026.

• 47 de 58 amenazas bloqueadas · 24 críticas

CLIENTE	SERVICIO	PERIODO
SWPanel Demo, S.L.	swpanel.com · 203.0.113.10	13-09-2026 a 12-10-2026 · 30 días
DOCUMENTO	**FECHA DE EMISIÓN**	**SENSIBILIDAD**
SW-NGF-EJEMPLO-2026	16-10-2026	Bloquea desde gravedad media

Contenido del informe

Cuadro de mando 2

01 Introducción del consultor 3

02 Amenazas 7
- Por gravedad, tipo y aplicación 8
- Las más repetidas, origen y destino 9
- Qué ha cambiado: los últimos 6 meses 10

03 Accesos y archivos 11
- Autenticación y archivos sospechosos 12

04 Qué hacer 13
- Las más graves primero 14

05 Detalle por host 16
- Host 203.0.113.10 17
- Qué es cada amenaza 19

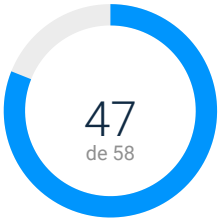
06 Conclusiones del análisis 22

Glosario 25

Anexo: cómputo de IA 27

Informe NGFW de swpanel.com generado por SWPanel

Cuadro de mando



81 % CON BLOQUEO

De los eventos detectados con acción de bloqueo, del 13-09-2026 al 12-10-2026

swpanel.com · 203.0.113.10 · bloquea desde gravedad media

11 de gravedad baja solo se registraron, como pide la sensibilidad.

• 24 críticas, todas bloqueadas

58	47	11	1	0
AMENAZAS DETECTADAS	BLOQUEADAS	REGISTRADAS	INTENTO DE ACCESO ILEGÍTIMO	ARCHIVOS SOSPECHOSOS

Por gravedad



• Crítica **24** • Alta **11** • Media **12** • Baja **11**

Frente a la media de los clientes

58
amenazas por host
Media: 944,7
93,9 % menos

1
intento de intrusión
Media: 659,9
99,8 % menos

0
archivos sospechosos
Media: 70,3
Ninguno

1
aplicación en la red
Media: 1,2
18,9 % menos

Lo que te conviene hacer

CRÍTICA

24 amenazas críticas, todas bloqueadas. Casi todas son de tipo «Ejecución de código». Mantén el servidor y sus programas actualizados.

REVISAR

11 amenazas solo se registraron. Son de gravedad baja y la sensibilidad bloquea desde gravedad media. Si quieres bloquearlas también, baja la sensibilidad en el panel.

1 intento(s) de fuerza bruta (WordPress Login Brute Force Attempt). Si usas WordPress, limita los intentos de acceso.

Informe NGFW de swpanel.com generado por SWPanel

Informe NGFW de swpanel.com generado por SWPanel

01

Introducción del consultor

Tu situación en un minuto, lo que hemos analizado y lo que merece tu atención.

Introducción del consultor

IA Escrito por el Asistente IA de seguridad de SWPanel

El firewall ha bloqueado 47 intentos de ataque en los últimos 30 días, con un enfoque en accesos no autorizados y vulnerabilidades en software.

ATENCIÓN

Tu situación en un minuto

Hay actividad maliciosa dirigida a tu servidor, pero el firewall ha actuado como barrera. Es importante revisar si el software que usas tiene vulnerabilidades conocidas.

1. Verifica si PHP 8.3 está actualizado, ya que hay un intento de ataque que sí afecta a tu servicio.

2. Revisa los logs de Cloudflare y de la aplicación para entender mejor el intento de ataque por fuerza bruta.

3. Considera activar la protección 'Seguridad 360' para tener más visibilidad y control sobre las amenazas.

Informe NGFW de swpanel.com generado por SWPanel

Lo que he analizado

He revisado el informe del firewall de los últimos 30 días, que incluye los intentos de ataque detectados y las conexiones rechazadas. El firewall está configurado para bloquear solo los eventos con severidad 'media' o superior, por lo que no todo lo que intenta acceder se detiene.

En este periodo, el firewall ha detectado 58 eventos de seguridad, de los cuales 47 han sido bloqueados. Esto indica que hay actividad maliciosa dirigida a tu servidor, pero el firewall ha actuado como barrera.

Lo que más llama la atención es que el 100% de los eventos con severidad 'alta' y 'crítica' han sido bloqueados, lo cual es positivo. Sin embargo, hay algunos intentos de ataque que no pudimos bloquear por política, y que también merecen atención.

También se registró un intento de ataque por fuerza bruta, aunque el origen está detrás de un proxy de Cloudflare, por lo que no sabemos con certeza quién lo realizó.

Tu Asistente IA de seguridad de SWPanel

¿Debo preocuparme?

Esto no significa que tu servidor esté comprometido, pero sí que hay intentos de ataque. El nivel de preocupación es moderado: hay actividad, pero el firewall ha actuado.

Introducción del consultor

Qué cubre este informe y qué no

Este informe muestra solo los intentos de ataque detectados y las conexiones rechazadas por el firewall. No incluye el tráfico normal permitido, el contenido de conexiones encriptadas ni lo que ocurre dentro del servidor.

Informe NGFW de swpanel.com generado por SWPanel

Lo que he encontrado y por qué importa

Cada hallazgo con lo que hemos visto, en qué nos basamos, qué significa para tu servicio, qué falta por comprobar, qué te recomendamos y cómo sabremos que está resuelto.

IMPACTO MEDIO

Intento de ataque a PHP 8.3

Qué hemos observado: Se detectaron 4 intentos de ataque relacionados con una vulnerabilidad en phpunit, que sí afecta a tu servicio si usas PHP 8.3.
En qué nos basamos: El firewall bloqueó estos intentos con severidad 'crítica'.
Qué significa: Si PHP 8.3 no está actualizado, podría ser explotado por atacantes.
Qué falta comprobar: No sabemos si PHP 8.3 está actualizado o si phpunit está instalado.
Qué recomendamos: Verifica si PHP 8.3 está actualizado y si phpunit está instalado y actualizado.
Cómo lo verificaremos: Comprueba las versiones instaladas de PHP y phpunit.

IMPACTO BAJO

Intento de ataque por fuerza bruta

Qué hemos observado: Se registró un intento de ataque por fuerza bruta al login de WordPress, desde un IP asociado a Cloudflare.
En qué nos basamos: El firewall bloqueó este intento.
Qué significa: Alguien intentó adivinar la contraseña de WordPress, pero no sabemos con certeza quién.
Qué falta comprobar: No sabemos si el ataque fue exitoso ni quién lo realizó.
Qué recomendamos: Revisa los logs de Cloudflare y de WordPress para ver si hubo más intentos y si el acceso fue exitoso.
Cómo lo verificaremos: Comprueba los logs de Cloudflare y de WordPress.

IMPACTO BAJO

Varios intentos de ataque no aplicables

Qué hemos observado: Se detectaron intentos de ataque relacionados con dispositivos IoT o routers, que no afectan a tu servidor web.
En qué nos basamos: El firewall bloqueó estos intentos con severidad 'crítica'.
Qué significa: Estos intentos no son relevantes para tu servicio actual.
Qué falta comprobar: No hay riesgo real para tu servidor con estos intentos.
Qué recomendamos: No es necesario actuar sobre estos intentos, pero puedes revisarlos si te interesa.
Cómo lo verificaremos: Revisa los eventos del firewall para confirmar que no afectan a tu servicio.

Informe NGFW de swpanel.com generado por SWPanel

Informe NGFW de swpanel.com generado por SWPanel

02

Amenazas

Qué ha llegado, de qué gravedad y tipo, por qué aplicación y desde dónde.

Amenazas del periodo

IA **El consultor opina**

Los intentos de ataque son frecuentes, pero el firewall ha actuado como barrera. Sin embargo, hay que prestar atención a los intentos que sí afectan a tu software.

El NGFW ha detectado 58 amenazas en el periodo. Ha bloqueado las 47 de gravedad media, alta o crítica y ha registrado sin bloquear las 11 de gravedad baja.

• 47 bloqueadas • 11 registradas

Por gravedad



• Crítica **24** • Alta **11** • Media **12** • Baja **11**

Por tipo

Tipo	Gravedades	Bloqueadas	Registradas	Total
Ejecución de código	• Crítica • Baja	**23**	**5**	28
Filtrado de información	• Alta • Media • Baja	**19**	**1**	20
Anomalía de protocolo	• Baja	**0**	**5**	5
Denegación de servicio	• Alta	**4**	**0**	4
Fuerza bruta	• Crítica	**1**	**0**	1
Total		47	11	58

Por aplicación

Aplicación	Bloqueadas	Registradas	Total	Del total
web-browsing	**37**	**5**	42	**72 %**
ftp	**0**	**6**	6	**10 %**
soap	**5**	**0**	5	**8,6 %**
ssl	**4**	**0**	4	**6,9 %**
portmapper	**1**	**0**	1	**1,7 %**

Informe NGFW de swpanel.com generado por SWPanel

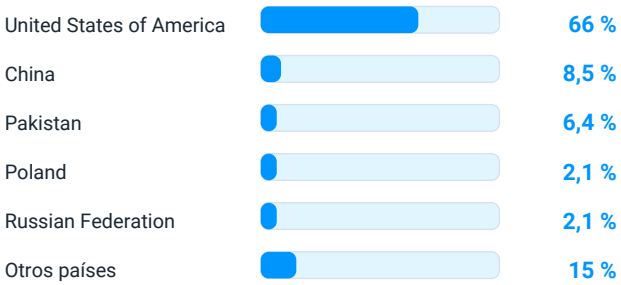
Las más repetidas, origen y destino

Las 10 más repetidas

Amenaza	Tipo	Gravedad	Intentos	Acción
HTTP /etc/passwd Access Attempt ID 35107 · web-browsing	**Filtrado de información**	• Alta	7	• Bloqueada
Apache Shiro Improper Authentication Vulnerability ID 58590 · web-browsing	**Ejecución de código**	• Crítica	6	• Bloqueada
HTTP Directory Traversal Request Attempt ID 30844 · web-browsing	**Filtrado de información**	• Media	6	• Bloqueada
D-Link DSL Soap Authorization Remote Command Execution Vulnerability ID 58483 · soap	**Ejecución de código**	• Crítica	5	• Bloqueada
FTP Protocol Evasion Application Detection ID 39826 · ftp	**Anomalía de protocolo**	• Baja	5	• Registrada
phpunit Remote Code Execution Vulnerability ID 55852 · web-browsing	**Ejecución de código**	• Crítica	4	• Bloqueada
Netgear DGN Device Remote Command Execution Vulnerability ID 40741 · web-browsing	**Ejecución de código**	• Crítica	4	• Bloqueada
OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability ID 58033 · ssl	**Denegación de servicio**	• Alta	4	• Bloqueada
ZGrab Application Layer Scanner Detection ID 57955 · web-browsing	**Filtrado de información**	• Media	4	• Bloqueada
GPON Home Routers Remote Code Execution Vulnerability ID 37264 · web-browsing	**Ejecución de código**	• Crítica	3	• Bloqueada

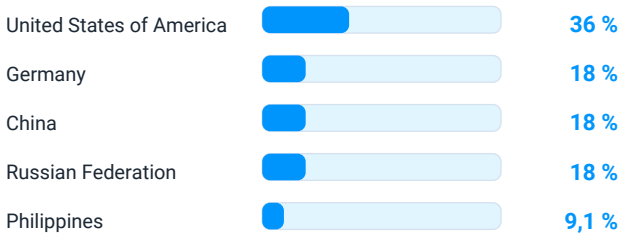
Origen de las bloqueadas

47 amenazas, por país



Origen de las registradas

11 amenazas, por país



Informe NGFW de swpanel.com generado por SWPanel

Las más repetidas, origen y destino (continuación)

Destino

Las 58 amenazas fueron a swpanel.com (203.0.113.10), el único servicio de este informe.

Qué ha cambiado: los últimos 6 meses

Mes	Eventos	Con bloqueo	Registrados	Críticos	Altos	Fuerza bruta
mayo 2026	**0**	0	0	0	0	0
junio 2026	**0**	0	0	0	0	0
julio 2026	**22**	11	11	11	0	0
agosto 2026	**51**	35	16	24	1	0
septiembre 2026	**92**	77	15	38	16	1
octubre 2026	**0**	0	0	0	0	0

Meses naturales; el último, hasta el final del periodo de este informe. Comparar con tu propio historial dice más que cualquier media.

Informe NGFW de swpanel.com generado por SWPanel

03

Accesos y archivos

Intentos de entrar a la fuerza y archivos sospechosos.

Informe NGFW de swpanel.com generado por SWPanel

Accesos y archivos sospechosos

IA **El consultor opina**

No se registraron accesos SSH ni archivos sospechosos, lo cual es positivo.

Intentos de acceso por fuerza bruta

El NGFW ha bloqueado 1 intento(s) de entrar a la fuerza, frente a 660 de media por host en el resto de clientes. Muchos de estos ataques son automáticos y se lanzan contra cualquier equipo conectado a internet: con el sistema al día, las aplicaciones bien configuradas y contraseñas seguras no suponen un riesgo real.

Amenaza	Servicio	IP de origen	Intentos	Acción
WordPress Login Brute Force Attempt ID 40044	**swpanel.com**	**198.51.100.26** Cloudflare (proxy)	1	• Bloqueada

Sesiones SSH

Nadie ha llegado a la pantalla de login de SSH en el periodo.

Archivos sospechosos

No se ha detectado ningún archivo sospechoso: ni bloqueado ni registrado. La media de los clientes es de 70 por host.

Informe NGFW de swpanel.com generado por SWPanel

Informe NGFW de swpanel.com generado por SWPanel

04

Qué hacer

Qué es cada tipo de amenaza detectada y cómo protegerte, por orden de lo que te juegas.

QUÉ HACER

Cómo protegerte

Solo los tipos que se han detectado en este periodo, de más a menos grave.

Ejecución de código · 28 intentos

• Crítica • Baja

Intentos de que el servidor ejecute órdenes del atacante. Un exploit o un ransomware entran en esta categoría y pueden comprometer todo el sistema. Llegaron a swpanel.com por soap, web-browsing; 8 amenaza(s) distinta(s).

QUÉ HACER

Filtra las amenazas en capa 7, instala un antivirus y mantén el servidor y sus programas actualizados.

Fuerza bruta · 1 intentos

• Crítica

Probar muchos usuarios y contraseñas seguidos hasta acertar. Llegaron a swpanel.com por web-browsing; 1 amenaza(s) distinta(s).

QUÉ HACER

Contraseñas seguras y bloqueo automático de las IPs que fallan varias veces seguidas, tanto en el cortafuegos como en el acceso a la aplicación.

Filtrado de información · 20 intentos

• Alta • Media • Baja

Intentos de sacar información interna del servidor: ficheros de configuración, contraseñas o datos personales. Llegaron a swpanel.com por ftp, portmapper, web-browsing; 6 amenaza(s) distinta(s).

QUÉ HACER

Que la información sensible no se pueda leer desde fuera: cifra los ficheros que la contienen y da permisos solo a los grupos de usuarios que la necesitan.

Denegación de servicio · 4 intentos

• Alta

Intentos de dejar un servicio sin respuesta, saturándolo o haciéndolo fallar. Llegaron a swpanel.com por ssl; 1 amenaza(s) distinta(s).

QUÉ HACER

Usa cortafuegos de capa 3 y de capa 7 para detectar y cortar las conexiones repetidas, y mantén actualizados los programas expuestos.

Informe NGFW de swpanel.com generado por SWPanel

QUÉ HACER

Cómo protegerte (continuación)

Anomalía de protocolo · 5 intentos • Baja

Tráfico que no se comporta como el protocolo que dice ser, normalmente para pasar desapercibido. Llegaron a swpanel.com por ftp; 1 amenaza(s) distinta(s).

QUÉ HACER

Cierra los puertos que no uses y deja que el NGFW identifique la aplicación antes de dejarla pasar: lo que no se reconoce, mejor bloquearlo.

Informe NGFW de swpanel.com generado por SWPanel

05

Detalle por host

Cada amenaza recibida por cada servicio, con su referencia.

Informe NGFW de swpanel.com generado por SWPanel

Host 203.0.113.10

IA El consultor opina

No hay datos sobre el software instalado, por lo que no podemos determinar con certeza si los intentos de ataque son relevantes.

swpanel.com ha recibido 58 amenazas de 17 tipos distintos, de más a menos grave.

ID	Amenaza	Gravedad	Intentos	Acción
58590	**Apache Shiro Improper Authentication Vulnerability** Ejecución de código · web-browsing	• Crítica	6	• Bloqueada
58483	**D-Link DSL Soap Authorization Remote Command Execution Vulnerability** Ejecución de código · soap	• Crítica	5	• Bloqueada
55852	**phpunit Remote Code Execution Vulnerability** Ejecución de código · web-browsing	• Crítica	4	• Bloqueada
40741	**Netgear DGN Device Remote Command Execution Vulnerability** Ejecución de código · web-browsing	• Crítica	4	• Bloqueada
37264	**GPON Home Routers Remote Code Execution Vulnerability** Ejecución de código · web-browsing	• Crítica	3	• Bloqueada
54617	**Mirai and Reaper Exploitation Traffic** Ejecución de código · web-browsing	• Crítica	1	• Bloqueada
40044	**WordPress Login Brute Force Attempt** Fuerza bruta · web-browsing	• Crítica	1	• Bloqueada
35107	**HTTP /etc/passwd Access Attempt** Filtrado de información · web-browsing	• Alta	7	• Bloqueada
58033	**OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability** Denegación de servicio · ssl	• Alta	4	• Bloqueada
30844	**HTTP Directory Traversal Request Attempt** Filtrado de información · web-browsing	• Media	6	• Bloqueada
57955	**ZGrab Application Layer Scanner Detection** Filtrado de información · web-browsing	• Media	4	• Bloqueada
32796	**RPC Portmapper DUMP Request Detected** Filtrado de información · portmapper	• Media	1	• Bloqueada
34804	**PHP CGI Query String Parameter Handling Information Disclosure Vulnerability** Filtrado de información · web-browsing	• Media	1	• Bloqueada
39826	**FTP Protocol Evasion Application Detection** Anomalía de protocolo · ftp	• Baja	5	• Registrada

Informe NGFW de swpanel.com generado por SWPanel

Host 203.0.113.10 (continuación)

ID	Amenaza	Gravedad	Intentos	Acción
58098	**Possible HTTP Malicious Payload Detection** Ejecución de código · web-browsing	• Baja	3	• Registrada
54469	**Suspicious File Downloading Detection** Ejecución de código · web-browsing	• Baja	2	• Registrada
40391	**Application Identification Evasion Attempt Through Malformed FTP Traffic** Filtrado de información · ftp	• Baja	1	• Registrada

Informe NGFW de swpanel.com generado por SWPanel

Qué es cada amenaza

ID 58590 · Ejecución de código • Crítica

Apache Shiro Improper Authentication Vulnerability

Apache Shiro es vulnerable a una autenticación inadecuada al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una vulnerabilidad de autenticación inadecuada explotable.

Intentos **6** Bloqueada CVE-2020-11989 Ref. **lists.apache.org**

ID 58483 · Ejecución de código • Crítica

D-Link DSL Soap Authorization Remote Command Execution Vulnerability

Dlink DSL es vulnerable a la inyección de comandos al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una inyección de comandos explotable.

Intentos **5** Bloqueada CVE-2018-19986 Ref. **github.com**

ID 55852 · Ejecución de código • Crítica

phpunit Remote Code Execution Vulnerability

phpunit es vulnerable a la ejecución de código remoto al procesar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una ejecución de código remoto explotable.

Intentos **4** Bloqueada CVE-2017-9841 Ref. **phpunit.vulnbusters.com**

ID 40741 · Ejecución de código • Crítica

Netgear DGN Device Remote Command Execution Vulnerability

Los dispositivos Netgear DGN son propensos a una vulnerabilidad de ejecución de código remoto al analizar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones de privilegios en la solicitud, lo que lleva a una vulnerabilidad de ejecución de código remoto exp...

Intentos **4** Bloqueada Ref. **seclists.org**

ID 37264 · Ejecución de código • Crítica

GPON Home Routers Remote Code Execution Vulnerability

Los routers de hogar GPON son propensos a una vulnerabilidad de ejecución de código remoto al analizar ciertas solicitudes HTTP elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes HTTP, lo que lleva a una vulnerabilidad de ejecución de código remoto exp...

Intentos **3** Bloqueada CVE-2018-10561 Ref. **blog.netlab.360.com**

ID 54617 · Ejecución de código • Crítica

Mirai and Reaper Exploitation Traffic

Esta firma detecta intentos de explotación de los malware Mirai y Reaper. La detección de este tráfico indica un intento de explotar diversas vulnerabilidades de dispositivos IoT, incluyendo: la vulnerabilidad de inyección de comandos del sistema operativo en D-Link DSL-2750B, la vulnerabilidad d...

Intentos **1** Bloqueada

Informe NGFW de swpanel.com generado por SWPanel

Qué es cada amenaza (continuación)

ID 40044 · Fuerza bruta • Crítica

WordPress Login Brute Force Attempt

Este evento indica que alguien está utilizando un ataque de fuerza bruta para acceder a WordPress wp-login.php.

Intentos **1** Bloqueada

ID 35107 · Filtrado de información • Alta

HTTP /etc/passwd Access Attempt

Se ha detectado un intento de acceso al archivo /etc/passwd al analizar ciertas solicitudes HTTP elaboradas. Un ataque exitoso podría permitir a un atacante acceder a información sensible que podría facilitar otros ataques.

Intentos **7** Bloqueada

ID 58033 · Denegación de servicio • Alta

OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability

OpenSSL es vulnerable a un error de referencia de puntero NULL al procesar ciertas solicitudes SSL elaboradas. La vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes SSL, lo que lleva a una vulnerabilidad de referencia de puntero NULL explotable.

Intentos **4** Bloqueada CVE-2020-1967 Ref. **openssl.org**

ID 30844 · Filtrado de información • Media

HTTP Directory Traversal Request Attempt

Se ha descubierto una vulnerabilidad de recorrido de directorios al analizar solicitudes HTTP malformadas. Esta vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes URI HTTP.

Intentos **6** Bloqueada Ref. **imperva.com**

ID 57955 · Filtrado de información • Media

ZGrab Application Layer Scanner Detection

Esta firma indica que un atacante está intentando recopilar información sobre la red utilizando el escáner ZGrab.

Intentos **4** Bloqueada

ID 32796 · Filtrado de información • Media

RPC Portmapper DUMP Request Detected

La mayoría de los servidores Unix pueden obtener información mediante una solicitud normal al puerto de mapeo de puertos.

Intentos **1** Bloqueada

ID 34804 · Filtrado de información • Media

PHP CGI Query String Parameter Handling Information Disclosure Vulnerability

Las configuraciones basadas en PHP-CGI, como Apache's mod_cgid, contienen una vulnerabilidad al analizar parámetros de cadena de consulta de archivos PHP. En este tipo de configuración, php-cgi recibe una cadena de consulta procesada como argumentos de línea de comandos, lo que permite pasar opci...

Intentos **1** Bloqueada CVE-2012-1823 Ref. **kb.cert.org**

ID 39826 · Anomalía de protocolo • Baja

FTP Protocol Evasion Application Detection

Esta firma detecta aplicaciones o herramientas que tunnelean el tráfico SSH a través del tráfico FTP.

Intentos **5** Registrada Ref. **room362.com**

Informe NGFW de swpanel.com generado por SWPanel

Qué es cada amenaza (continuación)

ID 58098 · Ejecución de código • Baja

Possible HTTP Malicious Payload Detection

Esta firma detecta una carga útil maliciosa en el tráfico HTTP.

Intentos **3** Registrada Ref. **unit42.paloaltonetworks.com**

ID 54469 · Ejecución de código • Baja

Suspicious File Downloading Detection

Esta firma detecta la ejecución de comandos WGET y CURL en parámetros de URL de solicitudes HTTP, lo cual es ampliamente explotado por atacantes para obtener posteriormente una carga útil maliciosa.

Intentos **2** Registrada

ID 40391 · Filtrado de información • Baja

Application Identification Evasion Attempt Through Malformed FTP Traffic

La firma detecta un intento de evasión de identificación de aplicaciones que envía tráfico malformado a través del puerto TCP 21.

Intentos **1** Registrada Ref. **jira-hq.paloaltonetworks.local**

Informe NGFW de swpanel.com generado por SWPanel

06

Conclusiones del análisis

Lo que concluye tu consultor después de ver todas las cifras, y tu plan de acción.

Informe NGFW de swpanel.com generado por SWPanel

Conclusiones del análisis

IA **Escrito por el Asistente IA de seguridad de SWPanel**

El firewall ha bloqueado la mayoría de los intentos de ataque detectados, especialmente aquellos con alto o crítico nivel de gravedad. Esto indica que la protección está funcionando como se espera.

En comparación con el periodo anterior, el número total de eventos ha disminuido, aunque siguen siendo frecuentes los intentos de explotar vulnerabilidades en software, como PHP.

Aunque no se observaron accesos SSH ni archivos sospechosos, sí hubo un intento de ataque por fuerza bruta. Es importante revisar los logs internos para asegurarse de que no haya actividad inesperada.

Queda pendiente verificar si PHP 8.3 y phpunit están actualizados, ya que son aplicables a tu servicio. Además, aunque algunos intentos no son relevantes, siempre es bueno estar alerta.

Tu plan de acción

ESTE MES
Verificar si PHP 8.3 y phpunit están actualizados
Por qué: Hay intentos de ataque aplicables a estos componentes, y mantenerlos actualizados reduce el riesgo de explotación.
Quién: Tú
Cómo lo comprobaremos: Comprueba las versiones instaladas desde SWPanel o mediante el soporte técnico.

ESTE MES
Revisar los logs de Cloudflare y WordPress tras el intento de fuerza bruta
Por qué: El ataque fue bloqueado, pero es útil confirmar si hubo más intentos o si el acceso fue exitoso en algún momento.
Quién: Tú
Cómo lo comprobaremos: Consulta los registros de acceso de WordPress y los logs de Cloudflare para ver si hay actividad sospechosa.

MEDIO PLAZO
Considerar activar Seguridad 360 para una protección más completa
Por qué: Añadirá un WAF adaptativo, bloqueo de bots, control por país y monitoreo activo, lo que cubriría mejor las amenazas detectadas.
Quién: Tú
Cómo lo comprobaremos: Activa el servicio desde SWPanel y revisa las nuevas reglas y alertas en los próximos informes.

Informe NGFW de swpanel.com generado por SWPanel

Conclusiones del análisis

Seguridad 360: un paso más

PRUÉBALO

Con Seguridad 360, podrías contar con un WAF adaptativo, bloqueo de bots, control por país y un SOC que vigila las amenazas en tiempo real. Esto cubriría mejor las vulnerabilidades detectadas y ofrecería protección proactiva. Puedes probarlo desde SWPanel en cualquier momento.

Estamos aquí para ayudarte a mantener tu servicio seguro. Si tienes dudas o necesitas apoyo, no dudes en contactarnos desde SWPanel.

Tu Asistente IA de seguridad de SWPanel

Texto redactado por el Asistente IA de SWPanel a partir de los datos de este informe, con un modelo que funciona en servidores propios de SW Hosting: tus datos no salen de nuestra infraestructura. Las cifras las calcula el sistema; la IA solo las interpreta.

Informe NGFW de swpanel.com generado por SWPanel

Glosario

Los términos técnicos que salen en este informe, por orden alfabético.

Amenaza bloqueada
La que el NGFW ha detenido antes de llegar al servidor, según la sensibilidad elegida.

Amenaza registrada
La que se ha detectado y anotado pero no bloqueado, porque su gravedad está por debajo de la sensibilidad.

Anomalía de protocolo
Tráfico que no se comporta como el protocolo que dice ser.

Aplicación
Tipo de tráfico que el NGFW reconoce por su contenido (web-browsing, ssl, ftp…), no solo por el puerto.

CVE
Código público que identifica una vulnerabilidad conocida, por ejemplo CVE-2020-1967.

Denegación de servicio
Ataque que satura o hace fallar un servicio hasta que deja de responder.

Ejecución de código
Ataque que intenta que el servidor ejecute órdenes del atacante.

Exploit
Programa o petición que aprovecha una vulnerabilidad concreta.

Filtrado de información
Intento de sacar datos internos del servidor, como ficheros de configuración o contraseñas.

Fuerza bruta
Probar muchas contraseñas seguidas hasta acertar.

Gravedad
Nivel de riesgo de una amenaza: crítica, alta, media o baja.

ID de amenaza
Identificador de la amenaza en el catálogo del fabricante del NGFW.

Informe NGFW de swpanel.com generado por SWPanel

Glosario (continuación)

Inyección SQL
Colar órdenes de base de datos en los datos que se envían a una aplicación.

NGFW
Next Generation Firewall: cortafuegos que analiza el contenido del tráfico para detectar y bloquear amenazas.

Sensibilidad
Gravedad a partir de la cual el NGFW bloquea. Por debajo, solo registra.

Sesión
Una conexión completa entre dos equipos, del primer paquete al último.

Tráfico de entrada y de salida
Los datos que llegan a tus servicios y los que salen de ellos.

Vulnerabilidad
Fallo de seguridad de un programa que un atacante puede aprovechar.

Informe NGFW de swpanel.com generado por SWPanel

Anexo: cómputo de IA

IA **Lo que ha costado escribir este informe con IA**

El asistente y las traducciones de este informe los ha generado un modelo de lenguaje que funciona en servidores propios de SW Hosting: tus datos no salen de nuestra infraestructura.

Cómputo de IA

qwen3-32b MODELO	**vLLM** MOTOR	**3** LLAMADAS AL MODELO
6.476 TOKENS LEÍDOS	**3.182** TOKENS ESCRITOS	**73,1 s** TIEMPO DE CÓMPUTO

Infraestructura

NVIDIA A100 GPU	**80 GB** HBM2E	**312 TFLOPS** FP16/BF16

Energía y coste

0,0117 kWh CONSUMO DE CÓMPUTO	**0,0292 kWh** CONSUMO TOTAL (CON REFRIGERACIÓN)	**7,3 g** CO2 EMITIDO
0,0419 € COSTE DE CÓMPUTO		

Estimación: GPU a 575 W, refrigeración de 1,5 kW por kW de cómputo, 0,185 EUR/kWh, 1,8 EUR por hora de GPU y 250 g de CO2 por kWh.

Informe NGFW de swpanel.com generado por SWPanel

swpanel

https://www.swpanel.com

Documento: SW-NGF-EJEMPLO-2026

Informe generado automáticamente por SWPanel · https://www.swpanel.com