swpanel

SEGURETAT 360 · SOC · NGFW

Informe de Seguretat 360
swpanel.com

El que el tallafoc NGFW ha detectat i bloquejat a swpanel.com (203.0.113.10) del 13 de setembre al 12 d'octubre de 2026.

• 47 de 58 amenaces bloquejades · 24 crítiques

CLIENT	SERVEI	PERÍODE
SWPanel Demo, S.L.	swpanel.com · 203.0.113.10	13-09-2026 a 12-10-2026 · 30 dies
DOCUMENT	**DATA D'EMISSIÓ**	**SENSIBILITAT**
SW-S36-EJEMPLO-2026	16-10-2026	Bloqueja des de gravetat mitjana

Contingut de l'informe

Quadre de comandament 2

01 Introducció del consultor 3

02 Amenaces 7
- Per gravetat, tipus i aplicació 8
- Les més repetides, origen i destí 9
- Què ha canviat: els darrers 6 mesos 10

03 Accessos i arxius 11
- Autenticació i arxius sospitosos 12

04 Què fer 13
- Les més greus primer 14

05 Detall per host 16
- Host 203.0.113.10 17
- Què és cada amenaça 19

06 Seguretat 360 22
- Diagnòstic de Seguretat 360 23
- SOC: troballes obertes 25
- Accessos i canvis sensibles 26
- Bloqueig per països 27
- Bloqueig de bots 28
- Anàlisi de codi 29
- WAF adaptatiu 30
- Què s'ha fet al període 31
- Què hem fet per tu 32
- Recursos i disponibilitat creuats amb la seguretat 33
- Riscos pendents i què decidir 34
- Pla del proper mes 35

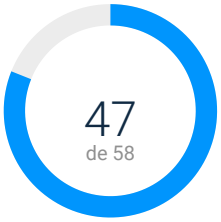
07 Conclusions de l'anàlisi 37

Glossari 40

Annex: còmput d'IA 42

Informe NGFW de swpanel.com generat per SWPanel

Quadre de comandament



81 % AMB BLOQUEIG

Dels esdeveniments detectats amb acció de bloqueig, del 13-09-2026 al 12-10-2026

swpanel.com · 203.0.113.10 · bloqueja des de gravetat mitjana

11 de gravetat baixa només es van registrar, com demana la sensibilitat.

• 24 crítiques, totes bloquejades

58	47	11	1	0
AMENACES DETECTADES	BLOQUEJADES	REGISTRADES	INTENT D'ACCÉS IL·LEGAL	ARXIUS SOSPITOSOS

Per gravetat



• Crítica **24** • Alta **11** • Mitjana **12** • Baixa **11**

Davant de la mitjana dels clients

58
amenaces per host
Mitjana: 944,7
93,9 % menys

1
intent d'intrusió
Mitjana: 659,9
99,8 % menys

0
arxius sospitosos
Mitjana: 70,3
Cap

1
aplicació a la xarxa
Mitjana: 1,2
18,9 % menys

El que et convé fer

CRÍTICA

24 amenaces crítiques, totes bloquejades. Gairebé totes són del tipus «Execució de codi». Mantén el servidor i els seus programes actualitzats.

REVISAR

11 amenaces només es van registrar. Són de gravetat baixa i la sensibilitat bloqueja des de gravetat mitjana. Si vols bloquejar-les també, baixa la sensibilitat al panell.

1 intent(s) de força bruta (WordPress Login Brute Force Attempt). Si fas servir WordPress, limita els intents d'accés.

Informe NGFW de swpanel.com generat per SWPanel

01

Introducció del consultor

La teva situació en un minut, el que hem analitzat i el que mereix la teva atenció.

Informe NGFW de swpanel.com generat per SWPanel

Introducció del consultor

IA Escrit per l'Assistent IA de seguretat de SWPanel

El teu servei ha rebut 58 intents de seguretat en els últims 30 dies, 47 dels quals s'han bloquejat.

ATENCIÓ

La teva situació en un minut

S'han bloquejat 47 intents de seguretat, la majoria d'ells de severitat alta o crítica. Cal revisar si el teu entorn és vulnerable a aquests atacs.

1. Revisa si el teu entorn utilitza versions afectades de PHP 8.3, ja que s'ha detectat una vulnerabilitat aplicable.

2. Comprova els registres de Cloudflare per veure si l'IP 198.51.100.21 ha accedit amb èxit al teu lloc.

3. Revisa el llistat d'intents de vulnerabilitats per veure si el teu entorn web és compatible amb algun dels productes mencionats.

Informe NGFW de swpanel.com generat per SWPanel

El que he analitzat

He revisat el report de la teva firewall de la darrera setmana, que mostra els intents de seguretat detectats i els bloquejos aplicats.

El període ha estat tranquil comparat amb el mes anterior, però hi ha alguns punts que cal revisar, especialment perquè s'han detectat intents concrets de vulnerabilitats.

El nivell de preocupació és moderat: no hi ha senyals d'una intrusió activa, però cal estar atent amb alguns riscos concrets.

A continuació, t'explico què hem vist i què pots fer ara.

El teu Assistent IA de seguretat de SWPanel

M'he de preocupar?

No cal alarmar-se, però sí estar atent. El nivell de risc és moderat: s'han bloquejat intents concrets, però no hi ha senyals d'una intrusió activa.

Què cobreix aquest informe i què no

Aquest report mostra només els intents de seguretat detectats i els bloquejos aplicats per la firewall. No inclou el tràfic normal ni el que passa dins del servidor.

El que he trobat i per què importa

Cada troballa amb el que hem vist, en què ens basem, què significa per al teu servei, què falta per comprovar, què et recomanem i com sabrem que està resolt.

IMPACTE ALT

Vulnerabilitat de phpunit detectada

Què hem observat: S'ha detectat un atac contra una vulnerabilitat de phpunit, que és aplicable al teu entorn si utilitzes PHP 8.3.

En què ens basem: Threat event: 'phpunit Remote Code Execution Vulnerability' (critical, block, 4 times).

Què significa: Aquesta vulnerabilitat permet executar codi remot si el teu entorn és vulnerable. És important revisar si la teva versió de PHP 8.3 és afectada.

Què falta comprovar: No sabem si el teu entorn és vulnerable. Cal revisar la versió exacta de PHP i si phpunit està instal·lat.

Què recomanem: Revisa si el teu entorn utilitza una versió afectada de PHP 8.3 i actualitza si cal.

Com ho verificarem: Quan s'actualitzi la versió de PHP o es corregi la vulnerabilitat, aquest tipus d'intents deixaran de detectar-se.

IMPACTE MITJÀ

Intents de login de WordPress

Què hem observat: S'ha detectat un intent de força bruta contra WordPress des d'una IP de Cloudflare.

En què ens basem: Threat event: 'WordPress Login Brute Force Attempt' (high, block, 1 time).

Què significa: Alguna IP ha intentat accedir a WordPress amb força bruta, però l'IP real està darrere d'un proxy. No sabem si l'atac ha tingut èxit.

Què falta comprovar: No sabem si l'usuari o contrasenya eren correctes. Cal revisar els registres de l'aplicació.

Què recomanem: Comprova els registres de login de WordPress per veure si s'ha produït cap accés no autoritzat.

Com ho verificarem: Si no hi ha cap accés no autoritzat en els registres, aquest incident estarà resolt.

Informe NGFW de swpanel.com generat per SWPanel

El que he trobat i per què importa

IMPACTE BAIX

Intents de vulnerabilitats sense aplicabilitat clara

Què hem observat: S'han detectat diversos intents contra vulnerabilitats de productes que no sembla que estiguin instal·lats al teu entorn.

En què ens basem: Threat events: Apache Shiro, D-Link DSL, Netgear DGN, OpenSSL, etc.

Què significa: Aquests intents no tenen aplicabilitat clara al teu entorn, però són senyals que s'han intentat atacs concrets.

Què falta comprovar: No sabem si aquests productes estan instal·lats o si són aplicables.

Què recomanem: Revisa si el teu entorn web utilitza algun dels productes o versions mencionats.

Com ho verificarem: Quan s'identifiqui si aquests productes estan instal·lats i si són vulnerables, es podran corregir.

Informe NGFW de swpanel.com generat per SWPanel

Informe NGFW de swpanel.com generat per SWPanel

02

Amenaces

Què ha arribat, de quina gravetat i tipus, per quina aplicació i des d'on.

Amenaces del període

IA **El consultor opina**

S'han detectat 58 intents de seguretat, la majoria de severitat alta o crítica. Aquestes són senyals que s'han intentat atacs concrets, però no hi ha senyals d'una intrusió activa.

El NGFW ha detectat 58 amenaces en el període. Ha bloquejat les 47 de gravetat mitjana, alta o crítica i ha registrat sense bloquejar les 11 de gravetat baixa.

• 47 bloquejades • 11 registrades

Per gravetat



• Crítica **24** • Alta **11** • Mitjana **12** • Baixa **11**

Per tipus

Tipus	Gravetats	Bloquejades	Registrades	Total
Execució de codi	• Crítica • Baixa	**23**	**5**	28
Filtratge d'informació	• Alta • Mitjana • Baixa	**19**	**1**	20
Anomalia de protocol	• Baixa	**0**	**5**	5
Denegació de servei	• Alta	**4**	**0**	4
Força bruta	• Crítica	**1**	**0**	1
Total		47	11	58

Per aplicació

Aplicació	Bloquejades	Registrades	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 generat per SWPanel

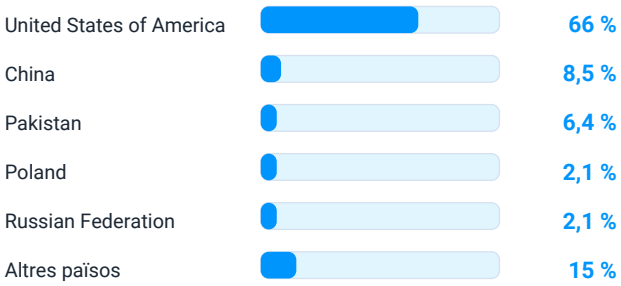
Les més repetides, origen i destí

Les 10 més repetides

Amenaça	Tipus	Gravetat	Intents	Acció
HTTP /etc/passwd Access Attempt ID 35107 · web-browsing	**Filtratge d'informació**	• Alta	7	• Bloquejada
Apache Shiro Improper Authentication Vulnerability ID 58590 · web-browsing	**Execució de codi**	• Crítica	6	• Bloquejada
HTTP Directory Traversal Request Attempt ID 30844 · web-browsing	**Filtratge d'informació**	• Mitjana	6	• Bloquejada
D-Link DSL Soap Authorization Remote Command Execution Vulnerability ID 58483 · soap	**Execució de codi**	• Crítica	5	• Bloquejada
FTP Protocol Evasion Application Detection ID 39826 · ftp	**Anomalia de protocol**	• Baixa	5	• Registrada
phpunit Remote Code Execution Vulnerability ID 55852 · web-browsing	**Execució de codi**	• Crítica	4	• Bloquejada
Netgear DGN Device Remote Command Execution Vulnerability ID 40741 · web-browsing	**Execució de codi**	• Crítica	4	• Bloquejada
OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability ID 58033 · ssl	**Denegació de servei**	• Alta	4	• Bloquejada
ZGrab Application Layer Scanner Detection ID 57955 · web-browsing	**Filtratge d'informació**	• Mitjana	4	• Bloquejada
GPON Home Routers Remote Code Execution Vulnerability ID 37264 · web-browsing	**Execució de codi**	• Crítica	3	• Bloquejada

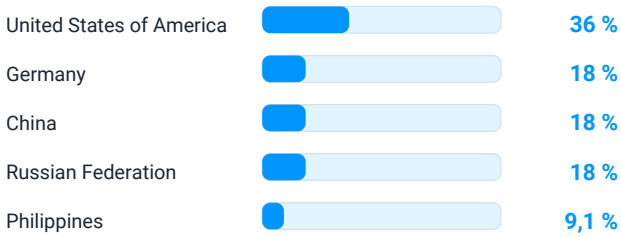
Origen de les bloquejades

47 amenaces, per país



Origen de les registrades

11 amenaces, per país



Informe NGFW de swpanel.com generat per SWPanel

Les més repetides, origen i destí (continuació)

Destí

Les 58 amenaces van anar a swpanel.com (203.0.113.10), l'únic servei d'aquest informe.

Què ha canviat: els darrers 6 mesos

Mes	Esdeveniments	Amb bloqueig	Registrats	Crítics	Alts	Força bruta
maig 2026	**0**	0	0	0	0	0
juny 2026	**0**	0	0	0	0	0
juliol 2026	**22**	11	11	11	0	0
agost 2026	**51**	35	16	24	1	0
setembre 2026	**92**	77	15	38	16	1
octubre 2026	**0**	0	0	0	0	0

Mesos naturals; el darrer, fins al final del període d'aquest informe. Comparar amb el teu propi historial diu més que qualsevol mitjana.

Informe NGFW de swpanel.com generat per SWPanel

Informe NGFW de swpanel.com generat per SWPanel

03

Accessos i arxius

Intents d'entrar per la força i arxius sospitosos.

Accessos i arxius sospitosos

IA El consultor opina

No s'han detectat sessions SSH ni intents de força bruta massius. Això és bo, però cal estar atent amb els intents de login de WordPress.

Intents d'accés per força bruta

El NGFW ha bloquejat 1 intent(s) d'entrar per la força, davant de 660 de mitjana per host a la resta de clients. Molts d'aquests atacs són automàtics i es llancen contra qualsevol equip connectat a internet: amb el sistema al dia, les aplicacions ben configurades i contrasenyes segures no suposen un risc real.

Amenaça	Servei	IP d'origen	Intents	Acció
WordPress Login Brute Force Attempt ID 40044	**swpanel.com**	**198.51.100.21** Cloudflare (proxy)	1	• Bloquejada

Sessions SSH

Ningú ha arribat a la pantalla de login de SSH en el període.

Arxius sospitosos

No s'ha detectat cap arxiu sospitós: ni bloquejat ni registrat. La mitjana dels clients és de 70 per host.

Informe NGFW de swpanel.com generat per SWPanel

04

Què fer

Què és cada tipus d'amenaça detectada i com protegir-te, per ordre del que t'hi jugues.

QUÈ FER

Com protegir-te

Només els tipus que s'han detectat en aquest període, de més a menys greu.

Execució de codi · 28 intents

• Crítica • Baixa

Intents que el servidor executi ordres de l'atacant. Un exploit o un ransomware entren en aquesta categoria i poden comprometre tot el sistema. Van arribar a swpanel.com per soap, web-browsing; 8 amenaça(es) diferent(s).

QUÈ FER

Filtra les amenaces en capa 7, instal·la un antivirus i mantén el servidor i els seus programes actualitzats.

Força bruta · 1 intents

• Crítica

Provar molts usuaris i contrasenyes seguits fins a encertar. Van arribar a swpanel.com per web-browsing; 1 amenaça(es) diferent(s).

QUÈ FER

Contrasenyes segures i bloqueig automàtic de les IPs que fallen diverses vegades seguides, tant al tallafoc com a l'accés a l'aplicació.

Filtratge d'informació · 20 intents

• Alta • Mitjana • Baixa

Intents de treure informació interna del servidor: fitxers de configuració, contrasenyes o dades personals. Van arribar a swpanel.com per ftp, portmapper, web-browsing; 6 amenaça(es) diferent(s).

QUÈ FER

Que la informació sensible no es pugui llegir des de fora: xifra els fitxers que la contenen i dona permisos només als grups d'usuaris que la necessiten.

Denegació de servei · 4 intents

• Alta

Intents de deixar un servei sense resposta, saturant-lo o fent-lo fallar. Van arribar a swpanel.com per ssl; 1 amenaça(es) diferent(s).

QUÈ FER

Fes servir tallafocs de capa 3 i de capa 7 per detectar i tallar les connexions repetides, i mantén actualitzats els programes exposats.

Informe NGFW de swpanel.com generat per SWPanel

Com protegir-te (continuació)

Anomalia de protocol · 5 intents • Baixa

Tràfic que no es comporta com el protocol que diu ser, normalment per passar desapercebut. Van arribar a swpanel.com per ftp; 1 amenaça(es) diferent(s).

QUÈ FER

Tanca els ports que no facis servir i deixa que el NGFW identifiqui l'aplicació abans de deixar-la passar: el que no es reconeix, millor bloquejar-ho.

Informe NGFW de swpanel.com generat per SWPanel

05

Detall per host

Cada amenaça rebuda per cada servei, amb la seva referència.

Host 203.0.113.10

IA El consultor opina

No s'han detectat arxius sospitosos ni sessions de login no autoritzades. Això és una bona senyal, però cal revisar els intents de login de WordPress.

swpanel.com ha rebut 58 amenaces de 17 tipus diferents, de més a menys greu.

ID	Amenaça	Gravetat	Intents	Acció
58590	**Apache Shiro Improper Authentication Vulnerability** Execució de codi · web-browsing	• Crítica	6	• Bloquejada
58483	**D-Link DSL Soap Authorization Remote Command Execution Vulnerability** Execució de codi · soap	• Crítica	5	• Bloquejada
55852	**phpunit Remote Code Execution Vulnerability** Execució de codi · web-browsing	• Crítica	4	• Bloquejada
40741	**Netgear DGN Device Remote Command Execution Vulnerability** Execució de codi · web-browsing	• Crítica	4	• Bloquejada
37264	**GPON Home Routers Remote Code Execution Vulnerability** Execució de codi · web-browsing	• Crítica	3	• Bloquejada
54617	**Mirai and Reaper Exploitation Traffic** Execució de codi · web-browsing	• Crítica	1	• Bloquejada
40044	**WordPress Login Brute Force Attempt** Força bruta · web-browsing	• Crítica	1	• Bloquejada
35107	**HTTP /etc/passwd Access Attempt** Filtratge d'informació · web-browsing	• Alta	7	• Bloquejada
58033	**OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability** Denegació de servei · ssl	• Alta	4	• Bloquejada
30844	**HTTP Directory Traversal Request Attempt** Filtratge d'informació · web-browsing	• Mitjana	6	• Bloquejada
57955	**ZGrab Application Layer Scanner Detection** Filtratge d'informació · web-browsing	• Mitjana	4	• Bloquejada
32796	**RPC Portmapper DUMP Request Detected** Filtratge d'informació · portmapper	• Mitjana	1	• Bloquejada
34804	**PHP CGI Query String Parameter Handling Information Disclosure Vulnerability** Filtratge d'informació · web-browsing	• Mitjana	1	• Bloquejada
39826	**FTP Protocol Evasion Application Detection** Anomalia de protocol · ftp	• Baixa	5	• Registrada

Informe NGFW de swpanel.com generat per SWPanel

Host 203.0.113.10 (continuació)

ID	Amenaça	Gravetat	Intents	Acció
58098	**Possible HTTP Malicious Payload Detection** Execució de codi · web-browsing	• Baixa	3	• Registrada
54469	**Suspicious File Downloading Detection** Execució de codi · web-browsing	• Baixa	2	• Registrada
40391	**Application Identification Evasion Attempt Through Malformed FTP Traffic** Filtratge d'informació · ftp	• Baixa	1	• Registrada

Informe NGFW de swpanel.com generat per SWPanel

Què és cada amenaça

ID 58590 · Execució de codi • Crítica

Apache Shiro Improper Authentication Vulnerability

Apache Shiro és vulnerable a una vulnerabilitat d'autenticació inadequada durant l'anàlisi de certes sol·licituds HTTP elaborades. La vulnerabilitat és deguda a la manca de verificacions adequades sobre les sol·licituds HTTP, cosa que pot portar a una vulnerabilitat d'autenticació inadequada expl...

Intents **6** Bloquejada CVE-2020-11989 Ref. **lists.apache.org**

ID 58483 · Execució de codi • Crítica

D-Link DSL Soap Authorization Remote Command Execution Vulnerability

Dlink DSL és vulnerable a una vulnerabilitat d'injecció de comandes durant l'anàlisi de certes sol·licituds HTTP elaborades. La vulnerabilitat és deguda a la manca de verificacions adequades sobre les sol·licituds HTTP, cosa que pot portar a una vulnerabilitat d'injecció de comandes explotable.

Intents **5** Bloquejada CVE-2018-19986 Ref. **github.com**

ID 55852 · Execució de codi • Crítica

phpunit Remote Code Execution Vulnerability

phpunit és propens a una vulnerabilitat d'execució de codi remot mentre s'analen sol·licituds HTTP confeccionades. La vulnerabilitat és deguda a la manca de verificacions adequades en les sol·licituds HTTP, portant a una vulnerabilitat d'execució de codi remot explotable.

Intents **4** Bloquejada CVE-2017-9841 Ref. **phpunit.vulnbusters.com**

ID 40741 · Execució de codi • Crítica

Netgear DGN Device Remote Command Execution Vulnerability

Els dispositius DGN de Netgear són propensos a una vulnerabilitat d'execució de codi remot mentre s'analen sol·licituds HTTP confeccionades. La vulnerabilitat és deguda a la manca de verificacions de privilegis en la sol·licitud, portant a una vulnerabilitat d'execució de codi remot explotable.

Intents **4** Bloquejada Ref. **seclists.org**

ID 37264 · Execució de codi • Crítica

GPON Home Routers Remote Code Execution Vulnerability

Els routers d'obrador GPON són propensos a una vulnerabilitat d'execució de codi remot mentre s'analen sol·licituds HTTP confeccionades. La vulnerabilitat és deguda a la manca de verificacions adequades en les sol·licituds HTTP, portant a una vulnerabilitat d'execució de codi remot explotable.

Intents **3** Bloquejada CVE-2018-10561 Ref. **blog.netlab.360.com**

ID 54617 · Execució de codi • Crítica

Mirai and Reaper Exploitation Traffic

Aquesta signatura detecta intents d'explotació dels atacs de les famílies de malware Mirai i Reaper. La detecció d'aquest tràfic indica un intent d'explotar diverses vulnerabilitats de dispositius IoT, incloent-hi: la vulnerabilitat d'injecció de comandes del sistema operatiu en D-Link DSL-2750B,...

Intents **1** Bloquejada

Informe NGFW de swpanel.com generat per SWPanel

Què és cada amenaça (continuació)

ID 40044 · Força bruta • Crítica

WordPress Login Brute Force Attempt

Aquest esdeveniment indica que algú està fent servir un atac de força bruta per accedir al fitxer wp-login.php de WordPress.

Intents **1** Bloquejada

ID 35107 · Filtratge d'informació • Alta

HTTP /etc/passwd Access Attempt

S'ha detectat un intent d'accés a /etc/passwd mentre s'analen sol·licituds HTTP confeccionades. Un atac exitós podria permetre a un atacant accedir a informació sensible que podria llançar altres atacs.

Intents **7** Bloquejada

ID 58033 · Denegació de servei • Alta

OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability

OpenSSL és vulnerable a una vulnerabilitat de desreferència de punter NULL durant l'anàlisi de certes sol·licituds SSL elaborades. La vulnerabilitat és deguda a la manca de verificacions adequades sobre les sol·licituds SSL, cosa que pot portar a una vulnerabilitat de desreferència de punter NULL...

Intents **4** Bloquejada CVE-2020-1967 Ref. **openssl.org**

ID 30844 · Filtratge d'informació • Mitjana

HTTP Directory Traversal Request Attempt

S'ha descobert una vulnerabilitat de recorregut de directoris en analitzar sol·licituds HTTP malformades. Aquesta vulnerabilitat és deguda a la manca de verificacions adequades en les sol·licituds d'URI HTTP.

Intents **6** Bloquejada Ref. **imperva.com**

ID 57955 · Filtratge d'informació • Mitjana

ZGrab Application Layer Scanner Detection

Aquesta regla indica que un atacant està intentant recollir informació sobre la xarxa mitjançant l'escàner ZGrab.

Intents **4** Bloquejada

ID 32796 · Filtratge d'informació • Mitjana

RPC Portmapper DUMP Request Detected

La majoria dels servidors Unix poden recuperar informació a través d'una sol·licitud normal del portmapper.

Intents **1** Bloquejada

ID 34804 · Filtratge d'informació • Mitjana

PHP CGI Query String Parameter Handling Information Disclosure Vulnerability

Les configuracions basades en PHP-CGI, com ara Apache's mod_cgid, contenen una vulnerabilitat en l'anàlisi de paràmetres de cadena de consulta des de fitxers php. En aquesta configuració, php-cgi rep una cadena de consulta processada com a arguments de línia de comandes, permetent passar opcions ...

Intents **1** Bloquejada CVE-2012-1823 Ref. **kb.cert.org**

ID 39826 · Anomalia de protocol • Baixa

FTP Protocol Evasion Application Detection

Aquesta signatura detecta aplicacions o eines que tunel·listen el tràfic SSH a través del tràfic del protocol FTP.

Intents **5** Registrada Ref. **room362.com**

Informe NGFW de swpanel.com generat per SWPanel

Què és cada amenaça (continuació)

ID 58098 · Execució de codi • Baixa

Possible HTTP Malicious Payload Detection

Aquesta regla detecta una càrrega útil maliciosa en el trànsit HTTP.

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

ID 54469 · Execució de codi • Baixa

Suspicious File Downloading Detection

Aquesta signatura detecta l'execució de comandes WGET i CURL en paràmetres d'URL de sol·licituds HTTP, que és àmpliament explotada per atacants per obtenir posteriorment una càrrega maliciosa.

Intents **2** Registrada

ID 40391 · Filtratge d'informació • Baixa

Application Identification Evasion Attempt Through Malformed FTP Traffic

La signatura detecta un intent d'evitar la identificació d'aplicacions que envia tràfic malformat a través del port TCP 21.

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

Informe NGFW de swpanel.com generat per SWPanel

06

Seguretat 360

Totes les proteccions del teu servei: el seu estat, el que han vist i el que queda per resoldre.

Informe NGFW de swpanel.com generat per SWPanel

Diagnòstic de Seguretat 360

IA Escrit per l'Assistent IA de seguretat de SWPanel

ATENCIÓ MITJANA

El nivell és de medi perquè hi ha intents de seguretat, però no són massius ni crítics, i el cortafoc actua amb una bona taxa de bloqueig.

El teu servei ha rebut 58 intents de seguretat en el darrer mes, 47 dels quals s'han bloquejat. Això és molt per sota de la mitjana d'altres serveis, però indica que el cortafoc actua amb una sensibilitat mitjana.

Hi ha hagut 1 intent de força bruta contra WordPress, bloquejat. No hi ha hagut accés remot per SSH ni fitxers sospitosos detectats.

El percentatge de bloquejos és alt (81%) entre els intents detectats, però cal revisar si aquestes amenaces són aplicables al teu entorn, ja que moltes no s'han pogut verificar amb l'inventari del software.

La cobertura és parcial: el cortafoc està verificat, però altres proteccions com el WAF i el fail2ban no ho estan. No hi ha dades dels bots ni del bloqueig per països.

Estat de cada protecció

Ho decideix el sistema amb el que pot comprovar: configurat no és el mateix que funcionant.

OPERATIU I VERIFICAT

Tallafoc NGFW

OPERATIU I VERIFICAT

SOC: vigilància i troballes

SENSE COBERTURA

Bloqueig de bots

Informe NGFW de swpanel.com generat per SWPanel

Diagnòstic de Seguretat 360

SENSE COBERTURA
Bloqueig per països

SENSE COBERTURA
AntiDDoS

CONFIGURAT, SENSE VERIFICAR
Fail2Ban: bloqueig de qui falla en entrar

CONFIGURAT, SENSE VERIFICAR
WAF adaptatiu
modo observa: detecta y propone, no bloquea

OPERATIU I VERIFICAT
Accessos SSH

OPERATIU I VERIFICAT
Anàlisi de codi

Informe NGFW de swpanel.com generat per SWPanel

SOC: troballes obertes

IA **El consultor opina**

El SOC ha detectat 71 riscos oberts, incloent-hi la falta de protecció SPF i DMARC, que permeten que qualsevol envii correu en nom del teu domini.

0	4	13	38
CRÍTIQUES	ALTS	MITJANS	TROBALLES OBERTES

2	5	0	23
NOUS EN 7 DIES	RESOLTS EN 7 DIES	PICS EN 30 DIES	IPS BLOQUEJADES

Les troballes més greus

3
active_check · SWP01
Falta DMARC | Sin registro _dmarc: el dominio es facilmente suplantable en correos de phishing

3
ip_reputation · SWP01
198.51.100.77 | red de bots (spamhaus, riesgo critical) | 41 peticiones

3
ip_reputation · SWP01
198.51.100.82 | escaner conocido (abuseipdb, riesgo alto) | 18 peticiones

Informe NGFW de swpanel.com generat per SWPanel

SOC: troballes obertes

Accessos i canvis sensibles

IA El consultor opina

Hi ha hagut 1 accés remot a través de SSH, però no s'ha detectat cap accés no autoritzat ni cap ús de root amb contrasenya.

1	0	0	248
ACCESSOS SSH	DES D'IPS NO D'ADMINISTRACIÓ	ROOT AMB CONTRASENYA	INTENTS FALLITS

11	0	0
IPS AMB ERRORS	USUARIS NOUS	SUDO D'USUARIS NO ROOT

Informe NGFW de swpanel.com generat per SWPanel

Bloqueig per països

IA El consultor opina

El 32,6% del tràfic maliciós prové dels EUA, però no hi ha cap bloqueig activ per països. Això vol dir que no s'ha aplicat cap mesura de prevenció basada en la ubicació.

8.564	8.061	10.481	0
PETICIONS DE PERSONES	DE ROBOTS	D'ESCÀNERS	PAÏSOS BLOQUEJATS

Activitat per país

País	Persones	Robots	Escàners	Bloqueig
United States of America	2.517	2.887	4.855	—
Spain	710	1.934	1	—
France	961	23	1.301	—
Singapore	1.273	5	718	—
Japan	363	8	961	—
Korea, Republic of	14	960	22	—
Belgium	366	3	507	—
Hong Kong	131	361	225	—
Lithuania	214	4	477	—
Canada	180	96	365	—
India	69	331	214	—
Brazil	177	216	162	—
Netherlands	187	45	145	—
Germany	234	65	65	—

Peticions a les teves webs al període, per la ubicació de la IP. Un país bloquejat que continua rebent peticions després del bloqueig indica que el tall no s'aplica.

Informe NGFW de swpanel.com generat per SWPanel

Bloqueig de bots

IA El consultor opina

El perfil de bloqueig de bots està en B, però només s'han bloquejat 6 bots. Els escenaris A i C bloquejarien més bots, especialment de IA, sense afectar el tràfic útil.

3.361	2.830	2.643	2.532
PETICIONS DE PERSONES	DE BOTS CONEGUTS	DE ROBOTS SENSE CATALOGAR	D'ESCÀNERS

38	6	8	B
BOTS DETECTATS	BOTS BLOQUEJATS	AGENTS NOUS DESCOBERTS	PERFIL ACTUAL

Els bots detectats

Bot	Família	Peticions	Estat
GPTBot (OpenAI)	IAG	57	• Bloquejada
Meta-WebIndexer (Meta AI)	IAG	55	• Bloquejada
Googlebot	BUS	51	Permès
PerplexityBot	IAG	45	• Bloquejada
Bytespider (ByteDance)	IAG	34	• Bloquejada
AhrefsBot	SEO	32	Permès
ChatGPT-User	IAG	32	• Bloquejada
OnCrawl	SEO	31	Permès
ClaudeBot (Anthropic)	IAG	30	• Bloquejada
Kimi-SearchBot (Moonshot AI)	IAG	30	Permès
Qwenbot (Alibaba)	IAG	29	Permès
DuckAssistBot (DuckDuckGo)	IAG	29	Permès
Applebot	BUS	28	Permès
KimiBot (Moonshot AI)	IAG	27	Permès
YouBot (You.com)	IAG	26	Permès

Informe NGFW de swpanel.com generat per SWPanel

Bloqueig de bots

Els perfils de bloqueig i el que tallaria cadascun

Perfil	Bots que talla	Nous	Peticions	Els principals
A	2	2	184	
B · aconsellable	6	4	642	
C	11	5	1.415	

Anàlisi de codi

IA **El consultor opina**

L'anàlisi del codi no ha trobat errors ni fitxers sospitosos. El punt de seguretat és alt (86/100), però cal revisar si tots els components estan actualitzats.

86 PUNTUACIÓ DEL CODI	**1** TROBALLES DE SEGURETAT	**0** CRÍTICS	**0** FITXERS SOSPITOSOS
3 ERRORS DE CODI	**0** ERRORS SQL	**0** RESPOSTES 5XX	**PHP 8.3** VERSIÓ DE PHP

Darrera anàlisi completa: 16/10/2026 · 4 anàlisis al període.

Informe NGFW de swpanel.com generat per SWPanel

Bloqueig de bots

WAF adaptatiu

IA El consultor opina

El WAF està en mode protegeix, però no bloqueja automàticament. S'han detectat 72 intents de seguretat, però només 8 s'han corregit.

Només observa	aplica	7	20
MODE	AUTONOMIA DE LA IA	REGLES	TRETS EN OMBRA

OBSERVA

El WAF adaptatiu està en mode observació: detecta i proposa regles, però no bloqueja per si sol. Passa'l a automàtic si vols que actuï.

El que ha fet el WAF al període

Acció	Qui	Resultat	Vegades
hallazgo:alta	panel	abierto	72
hallazgo:no_visto	panel	corregido	8
hallazgo:visto	panel	abierto	7

Informe NGFW de swpanel.com generat per SWPanel

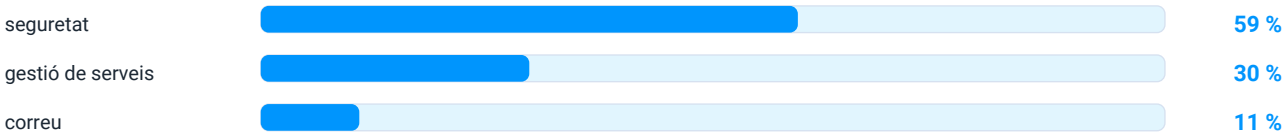
Què s'ha fet al període

IA El consultor opina

El SWPanel i la seva IA han actuat 64 vegades en el període, incloent 9 bloquejos d'IPs i 87 accions de WAF automàtiques.

64	11	4	0
ACCIONS REGISTRADES	FETES PER LA IA DE SWPANEL	PER API	IPS BLOQUEJADES AL FIREWALL

Per àrea



Les darreres accions

Data	Qui	Servei	Què
2026-10-14 09:12	**Titular**	SWP01	S'ha afegit la IP 203.0.113.50 (oficina) a la llista de permeses del FireWall.
2026-10-12 03:40	**SWPanel (IA)**	SWP01	El consultor d'IA ha preparat un informe dels bots que visiten el web. Perfil recomanat: B.
2026-10-11 18:05	**Titular**	SWP01	S'ha aplicat el perfil de bloqueig de bots B (6 bots bloquejats).
2026-10-09 02:15	**SWPanel**	SWP01	El WAF adaptatiu ha activat una regla contra rutes d'atac a /wp-login.php i /.env.
2026-10-07 11:30	**Titular**	SWP01	S'ha canviat la versió de PHP de 8.1 a 8.3.
2026-10-03 04:02	**SWPanel (IA)**	SWP01	El consultor d'IA ha preparat un informe del trànsit per països. Escenari recomanat: A.
2026-10-02 16:48	**API**	SWP01	Bloqueig de la IP 198.51.100.77 durant 24 hores per intents repetits d'accés.
2026-09-28 10:20	**Titular**	SWP01	S'ha renovat el certificat SSL de swpanel.com.
2026-09-22 08:15	**SWPanel**	SWP01	Còpia de seguretat completa verificada correctament.

Informe NGFW de swpanel.com generat per SWPanel

Què hem fet per tu

El que SWPanel, el seu SOC i la seva IA han fet pel teu servei al període, tret dels registres: no són intencions, són accions fetes.

9	87	5	4
IPS BLOQUEJADES PER SWPANEL	ACCIONS DEL WAF	TROBALLES RESOLTES (7 DIES)	ACCIONS AUTOMÀTIQUES RECENTS

Les darreres accions de SWPanel

Data	Qui	Què
2026-10-12 03:40	**SWPanel (IA)**	El consultor d'IA ha preparat un informe dels bots que visiten el web. Perfil recomanat: B.
2026-10-09 02:15	**SWPanel**	El WAF adaptatiu ha activat una regla contra rutes d'atac a /wp-login.php i /.env.
2026-10-03 04:02	**SWPanel (IA)**	El consultor d'IA ha preparat un informe del trànsit per països. Escenari recomanat: A.
2026-09-22 08:15	**SWPanel**	Còpia de seguretat completa verificada correctament.

Informe NGFW de swpanel.com generat per SWPanel

Recursos i disponibilitat creuats amb la seguretat

IA El consultor opina

El servei té recursos suficients: la CPU i la RAM no han arribat a límits, i no hi ha cap interrupció ni degradació de la disponibilitat.

1,1 % CPU MITJANA	**29 %** CPU MÀXIMA (MITJANA DIÀRIA)	**1,7 / 4** CÀRREGA MÀXIMA / VCORES	**49 %** RAM MÀXIMA
0 CAIGUDES	**0 min** TEMPS CAIGUT	**0** EPISODIS DE DEGRADACIÓ	**0** ATURADES PER SEGURETAT
0 HORES AL LÍMIT	**0** DE GRAVETAT ALTA	**0** RESPOSTES 5XX	**0** TIMEOUTS

L'encreuament: seguretat i rendiment

IA Escrit per l'Assistent IA de seguretat de SWPanel

No hi ha cap coincidència entre pics de tràfic i atacs o errors del codi. Això vol dir que els atacs no han causat cap problema visible en el funcionament del servei.

El tràfic de bots i escaners no ha generat cap pic de càrrega ni cap error 5xx. Els recursos del Cloud no han estat afectats per aquests intents de seguretat.

Informe NGFW de swpanel.com generat per SWPanel

Riscos pendents i què decidir

IA Escrit per l'Assistent IA de seguretat de SWPanel

IMPACTE ALT

Falta de protecció SPF i DMARC

Què hem observat: El SOC ha detectat que el teu domini no té registres SPF ni DMARC.
En què ens basem: Això permet que qualsevol envii correu en nom del teu domini, facilitant l'estafament i l'engany.
Què significa: És un risc alt per a la teva reputació i la seguretat dels teus usuaris.
Què falta comprovar: Cal afegir els registres SPF i DMARC al teu domini.
Què recomanem: Pots fer-ho a través del teu proveïdor de domini o demanar suport a SWPanel.
Com ho verificarem: Verifica que els registres SPF i DMARC apareixin a l'anàlisi del SOC.

IMPACTE MITJÀ

Falta de bloqueig per països

Què hem observat: No hi ha cap país bloquejat, tot i que el 32,6% del tràfic maliciós prové dels EUA.
En què ens basem: Això vol dir que no s'ha aplicat cap mesura preventiva basada en la ubicació.
Què significa: És un risc mitjà perquè no s'ha reduït el tràfic maliciós conegut.
Què falta comprovar: Cal considerar bloquejar països amb risc alt.
Què recomanem: Pots activar el bloqueig per països a través de SWPanel.
Com ho verificarem: Verifica que els països bloquejats apareixin a la configuració.

IMPACTE MITJÀ

Falta de bloqueig de bots de IA

Què hem observat: Hi ha hagut intents de bots de IA com GPTBot i Meta-WebIndexer, però només alguns s'han bloquejat.
En què ens basem: Aquests bots poden recopilar informació o generar tràfic no desitjat.
Què significa: És un risc mitjà perquè aquests bots poden afectar la disponibilitat i la seguretat.
Què falta comprovar: Cal revisar el perfil de bloqueig de bots.
Què recomanem: Considera passar a l'escenari C per bloquejar més bots de IA.
Com ho verificarem: Verifica que el perfil de bloqueig de bots sigui C.

Què hauries de decidir

Hauries de decidir si activar el bloqueig per països per reduir el tràfic maliciós conegut. L'alternativa és no fer-ho, però això pot deixar el servei exposat a intents coneguts.

Informe NGFW de swpanel.com generat per SWPanel

Pla del proper mes

AQUEST MES

Afegir els registres SPF i DMARC al domini.

Per què: Per evitar que qualsevol envii correu en nom del teu domini.

Qui: Tu

Com ho comprovarem: Verifica que els registres SPF i DMARC apareixin a l'anàlisi del SOC.

AQUEST MES

Activar el bloqueig per països.

Per què: Per reduir el tràfic maliciós conegut.

Qui: Tu

Com ho comprovarem: Verifica que els països bloquejats apareixin a la configuració.

AQUEST MES

Canviar el perfil de bloqueig de bots a C.

Per què: Per bloquejar més bots de IA i escaners.

Qui: Tu

Com ho comprovarem: Verifica que el perfil de bloqueig de bots sigui C.

MITJÀ TERMINI

Revisar la configuració del WAF.

Per què: Per assegurar que bloquegi automàticament els intents de seguretat.

Qui: Tu

Com ho comprovarem: Verifica que el WAF estigui en mode protegeix i que bloquegi automàticament.

MITJÀ TERMINI

Revisar l'inventari del software.

Per què: Per verificar si les amenaces detectades són aplicables al teu entorn.

Qui: Tu

Com ho comprovarem: Verifica que l'inventari del software sigui actualitzat.

Conclusions de Seguretat 360

El teu servei té una bona protecció bàsica, però hi ha espais per millorar, especialment en la gestió del correu i del tràfic de bots.

Informe NGFW de swpanel.com generat per SWPanel

Pla del proper mes

El cortafoc actua bé, però cal revisar si les amenaces detectades són aplicables al teu entorn i si s'han de bloquejar.

El SWPanel i la seva IA han actuat activament per protegir el servei, però cal que tu prenguis decisions clares per millorar la seguretat.

Informe NGFW de swpanel.com generat per SWPanel

07

Conclusions de l'anàlisi

El que conclou el teu consultor després de veure totes les xifres, i el teu pla d'acció.

Informe NGFW de swpanel.com generat per SWPanel

Conclusions de l'anàlisi

IA **Escrit per l'Assistent IA de seguretat de SWPanel**

El servei ha rebut menys intents de seguretat que el mes anterior, però encara s'han detectat 58 amenaces. Això mostra que la protecció està funcionant, però cal mantenir la vigilància.

Hi ha hagut intents concrets contra una vulnerabilitat de phpunit que sí que podria afectar el teu entorn. Aquest és un punt que cal revisar urgentment.

També s'ha detectat un únic intent de força bruta contra WordPress. Tot i que no s'ha pogut confirmar si ha sigut exitós, és recomanable revisar els registres del lloc.

Una part del tràfic bloquejat ha vingut dels Estats Units i Alemanya, però això no vol dir que hi hagi cap atacador concret. Són països amb molta activitat en línia.

Encara que el firewall ha bloquejat la majoria d'amenaces, hi ha hagut algunes que no s'han pogut avaluar per falta d'informació. Cal revisar l'entorn web per confirmar si són aplicables.

El teu pla d'acció

AQUESTA SETMANA

Revisar la versió de PHP 8.3 i actualitzar si cal.

Per què: Hi ha una vulnerabilitat de phpunit que afecta versions concretes de PHP 8.3.

Qui: Tu

Com ho comprovarem: Comprovar la versió actual de PHP a SWPanel i confirmar l'actualització.

AQUEST MES

Revisar els registres de login de WordPress per detectar accés no autoritzat.

Per què: S'ha detectat un intent de força bruta contra WordPress.

Qui: Tu

Com ho comprovarem: Comprovar que no hi hagi accés no autoritzat o canvis inusuals en el lloc.

Informe NGFW de swpanel.com generat per SWPanel

Conclusions de l'anàlisi

MITJÀ TERMINI

Revisar si el teu entorn web utilitza qualsevol dels productes o versions mencionats en les altres vulnerabilitats detectades.

Per què: Alguns intents podrien ser aplicables si s'utilitzen certes estructures o components.

Qui: Tu

Com ho comprovarem: Comprovar la configuració del lloc web i els components instal·lats a través de SWPanel.

Estem aquí per ajudar-te a revisar qualsevol detall o per fer una trucada per aclarir el que calgui. La teva seguretat és la nostra prioritat.

El teu Assistent IA de seguretat de SWPanel

Text redactat per l'Assistent IA de SWPanel a partir de les dades d'aquest informe, amb un model que funciona en servidors propis de SW Hosting: les teves dades no surten de la nostra infraestructura. Les xifres les calcula el sistema; la IA només les interpreta.

Informe NGFW de swpanel.com generat per SWPanel

Glossari

Els termes tècnics que surten en aquest informe, per ordre alfabètic.

Amenaça bloquejada
La que el NGFW ha aturat abans d'arribar al servidor, segons la sensibilitat escollida.

Amenaça registrada
La que s'ha detectat i anotat però no bloquejat, perquè la seva gravetat és inferior a la sensibilitat.

Anomalia de protocol
Tràfic que no es comporta com el protocol que diu ser.

Aplicació
Tipus de tràfic que el NGFW reconeix pel contingut (web-browsing, ssl, ftp), no només pel port.

CVE
Codi públic que identifica una vulnerabilitat coneguda, per exemple CVE-2020-1967.

Denegació de servei
Atac que satura o fa fallar un servei fins que deixa de respondre.

Execució de codi
Atac que intenta que el servidor executi ordres de l'atacant.

Exploit
Programa o petició que aprofita una vulnerabilitat concreta.

Filtratge d'informació
Intent de treure dades internes del servidor, com fitxers de configuració o contrasenyes.

Força bruta
Provar moltes contrasenyes seguides fins a encertar.

Gravetat
Nivell de risc d'una amenaça: crítica, alta, mitjana o baixa.

ID d'amenaça
Identificador de l'amenaça al catàleg del fabricant del NGFW.

Informe NGFW de swpanel.com generat per SWPanel

Glossari (continuació)

Injecció SQL
Colar ordres de base de dades a les dades que s'envien a una aplicació.

NGFW
Next Generation Firewall: tallafoc que analitza el contingut del tràfic per detectar i bloquejar amenaces.

Sensibilitat
Gravetat a partir de la qual el NGFW bloqueja. Per sota, només registra.

Sessió
Una connexió completa entre dos equips, del primer paquet a l'últim.

Tràfic d'entrada i de sortida
Les dades que arriben als teus serveis i les que en surten.

Vulnerabilitat
Error de seguretat d'un programa que un atacant pot aprofitar.

Informe NGFW de swpanel.com generat per SWPanel

Annex: còmput d'IA

IA **El que ha costat escriure aquest informe amb IA**

L'assistent i les traduccions d'aquest informe els ha generat un model de llenguatge que funciona en servidors propis de SW Hosting: les teves dades no surten de la nostra infraestructura.

Còmput d'IA

qwen3-32b MODEL	**vLLM** MOTOR	**3** CRIDES AL MODEL
6.455 TOKENS LLEGITS	**3.529** TOKENS ESCRITS	**71,0 s** TEMPS DE CÒMPUT

Infraestructura

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

Energia i cost

0,0113 kWh CONSUM DE CÒMPUT	**0,0283 kWh** CONSUM TOTAL (AMB REFRIGERACIÓ)	**7,1 g** CO2 EMÈS
0,0407 € COST DE CÒMPUT		

Estimació: GPU a 575 W, refrigeració d'1,5 kW per kW de còmput, 0,185 EUR/kWh, 1,8 EUR per hora de GPU i 250 g de CO2 per kWh.

Informe NGFW de swpanel.com generat per SWPanel

swpanel

https://www.swpanel.com

Document: SW-S36-EJEMPLO-2026

Informe generat automàticament per SWPanel · https://www.swpanel.com