swpanel

SEGURETAT AVANÇADA · NGFW

Informe d'amenaces 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-NGF-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

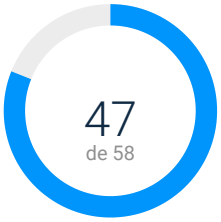
06 Conclusions de l'anàlisi 22

Glossari 25

Annex: còmput d'IA 27

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, la majoria bloquejats.

ATENCIÓ

La teva situació en un minut

Hi ha hagut intents de vulneracions reals i aplicables al teu entorn, sobretot en PHP. Cal actuar-hi.

1. Verifica la versió del PHP 8.3 per assegurar-te que no és vulnerable.
2. Revisa els registres de Cloudflare per veure si l'atac de força bruta contra WordPress va aconseguir res.
3. Comparteix amb nosaltres qualsevol aplicació o llibreria que s'utilitzi per revisar si cal actualitzar-la.

Informe NGFW de swpanel.com generat per SWPanel

El que he analitzat

He revisat el report de la teva firewall de la darrera setmana i he analitzat els 58 esdeveniments de seguretat detectats.

El nivell de sensibilitat de la firewall és 'mitjà', per tant, els esdeveniments de severitat mitjana o més altos han estat bloquejats, i els de severitat baixa només han estat registrats.

El que cal revisar ara són els intents de codi remot, especialment els que afecten el PHP 8.3 que ja saps que utilitzes.

No s'ha vist cap accés SSH ni cap fitxer sospitós, però sí un atac de força bruta contra WordPress.

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, i la majoria d'intents no són aplicables al teu entorn.

Què cobreix aquest informe i què no

Aquest report mostra només els intents de seguretat detectats i bloquejats per la firewall. No mostra 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

Intents de vulneració en PHP 8.3

Què hem observat: S'han detectat 4 intents d'execució de codi remot contra una vulnerabilitat de phpunit, bloquejats.
En què ens basem: Threat event: 'phpunit Remote Code Execution Vulnerability', 4 vegades.
Què significa: Aquesta vulnerabilitat afecta directament el teu entorn, ja que utilitzes PHP 8.3.
Què falta comprovar: Cal verificar si la teva versió de PHP 8.3 és afectada i si cal aplicar una actualització.
Què recomanem: Verifica la versió actual de PHP 8.3 i aplica les correccions si cal.
Com ho verificarem: Quan s'actualitzi la versió a una no afectada, ja no veurem aquest tipus d'intents.

IMPACTE MITJÀ

Atac de força bruta contra WordPress

Què hem observat: Un atac de força bruta contra WordPress ha estat bloquejat.
En què ens basem: Threat event: 'WordPress Login Brute Force Attempt', 1 vegada.
Què significa: Algui ha intentat endevinar contrasenyes d'administrador del teu lloc.
Què falta comprovar: Cal revisar si l'usuari afectat existeix i si s'ha intentat accedir-hi amb força.
Què recomanem: Revisa els registres de Cloudflare i de WordPress per veure si l'atac va aconseguir res.
Com ho verificarem: Si no hi ha intents de login fallits en els darrers dies, l'atac no ha aconseguit res.

Informe NGFW de swpanel.com generat per SWPanel

El que he trobat i per què importa

IMPACTE BAIX

Intents de vulneració no aplicables

Què hem observat: S'han bloquejat intents contra vulnerabilitats de dispositius IoT o routers, com D-Link o Netgear.

En què ens basem: Threat events: 'D-Link DSL Soap Authorization Remote Command Execution Vulnerability', 5 vegades; 'Netgear DGN Device Remote Command Execution Vulnerability', 4 vegades.

Què significa: Aquestes vulnerabilitats no afecten el teu entorn web, sinó dispositius de xarxa o IoT.

Què falta comprovar: No cal actuar-hi, però cal tenir-les en compte si s'afegeixen nous dispositius.

Què recomanem: No cal actuar-hi ara, però si afegeixes nous dispositius de xarxa, revisa les seves versions.

Com ho verificarem: Quan s'instal·lin nous dispositius, revisa si són afectats per aquestes vulnerabilitats.

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.

Informe NGFW de swpanel.com generat per SWPanel

Amenaces del període

IA **El consultor opina**

La majoria d'intents són reals i aplicables, però cal revisar quines afecten el teu entorn concret.

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

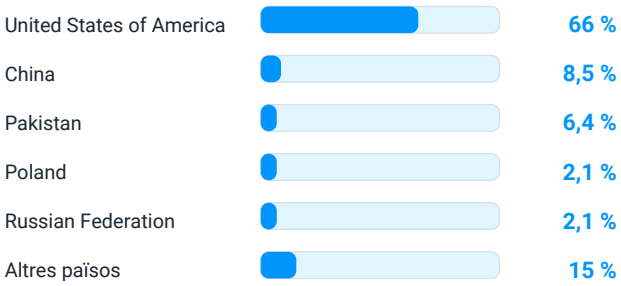
Les més repetides, origen i destí

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

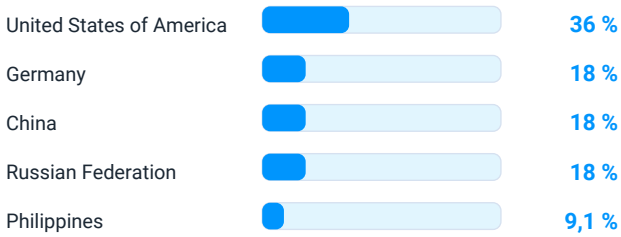
Origen de les bloquejades

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

03

Accessos i arxius

Intents d'entrar per la força i arxius sospitosos.

Accessos i arxius sospitosos

IA El consultor opina

No s'han vist accés SSH ni intents de forçar contrasenyes, però sí un atac de força bruta contra 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**	**198.51.100.26** 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.

Informe NGFW de swpanel.com generat per SWPanel

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.

Informe NGFW de swpanel.com generat per SWPanel

Host 203.0.113.10

IA **El consultor opina**

Tots els intents venen de IPs de Cloudflare, però no sabem quin usuari hi ha darrere. Revisa els logs d'aplicació.

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

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 teu servei ha rebut 58 intents de seguretat en els últims 30 dies, la majoria bloquejats. Aquesta xifra és més baixa que la del període anterior, però encara hi ha intents concrets que cal revisar.

Hi ha hagut un atac de força bruta contra WordPress, bloquejat, però cal revisar els registres per assegurar-se que no va aconseguir res. Aquest tipus d'atacs poden intentar adivinar contrasenyes.

Hi ha intents de vulneracions en PHP 8.3 que podrien afectar el teu servei. Cal confirmar si la versió actual és vulnerable i, en cas afirmatiu, actualitzar.

També hi ha intents de vulneracions que no semblen aplicables al teu entorn, com a atacs a enrutadors o dispositius IoT. No cal actuar-hi ara, però cal tenir-hi una mica d'atenció si afegeixes nous components.

En conjunt, el sistema de protecció està funcionant bé, però hi ha accions concretes que poden millorar la seguretat del teu servei.

El teu pla d'acció

AQUEST MES
Verificar la versió de PHP 8.3 i aplicar correccions si cal.
Per què: Hi ha intents de vulneració concrets en aquesta versió que podrien afectar el teu servei.
Qui: Tu
Com ho comprovarem: Comprovar la versió actual de PHP i confirmar si s'han aplicat les correccions.

AQUEST MES
Revisar els registres de Cloudflare i WordPress per veure si l'atac de força bruta va aconseguir res.
Per què: L'atac va ser bloquejat, però cal assegurar-se que no va deixar cap rastre.
Qui: Tu
Com ho comprovarem: Comprovar els registres de login de WordPress i els logs de Cloudflare.

Informe NGFW de swpanel.com generat per SWPanel

Conclusions de l'anàlisi

MITJÀ TERMINI

Activar Seguridad 360 per afegir capes addicionals de protecció.

Per què: Aquest paquet inclou un SOC, un WAF adaptatiu i bloqueig de bots, que poden millorar la seguretat del teu servei.

Qui: Tu

Com ho comprovarem: Confirmar l'activació de Seguridad 360 des de SWPanel.

Seguretat 360: un pas més

PROVA-HO

Amb Seguridad 360, el teu servei tindria una protecció més completa: un centre d'operacions de seguretat (SOC) que vigila en temps real, un parell de foc amb adaptació automàtica i bloqueig de bots. Aquestes capes addicionals podrien ajudar a prevenir molts dels intents que ja has rebut.

Estic aquí per ajudar-te a mantenir el teu servei segur i tranquil. Si tens qualsevol dubte, no dubtis a contactar-me.

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	**5** CRIDES AL MODEL
7.589 TOKENS LLEGITS	**5.258** TOKENS ESCRITS	**125,1 s** TEMPS DE CÒMPUT

Infraestructura

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

Energia i cost

0,0200 kWh CONSUM DE CÒMPUT	**0,0499 kWh** CONSUM TOTAL (AMB REFRIGERACIÓ)	**12,5 g** CO2 EMÈS
0,0718 € 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-NGF-EJEMPLO-2026

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