swpanel

ANÀLISI DE CODI I CORRECCIÓ AUTOMÀTICA · PREMIUM

Auditoria d'errors i correccions

Detecció i reparació d'errors de programació a partir dels logs d'Apache/Nginx.

Temps d'anàlisi: 6m 28s

DOMINI	ERRORS DETECTATS	FITXERS AFECTATS
swpanel.com (DEMO)	5 (2 crítics)	4
CORRECCIONS	**DATA**	**DOCUMENT**
4 / 4	16/10/2026	SW-COD-EJEMPLO-2026

S'analitzen els registres (logs) del 05-10-2026 al 12-10-2026

ÍNDEX

Índex

01 Resum executiu de seguretat **2**

02 Resum de l'anàlisi **5**

Introducció 6
Resum executiu 7
Errors detectats 8

03 Seguretat i detecció de programari maliciós **9**

Com funciona aquesta anàlisi 10
template-tags.php 11
functions.php 12
class-pricing.php 13
export.php 14

04 Correccions proposades **15**

template-tags.php 16
functions.php 18
class-pricing.php 20
export.php 22

05 Errors SQL detectats **24**

06 Diagnòstic del trànsit **26**

07 Trànsit i seguretat (logs d'accés) **30**

08 Errors de JavaScript **34**

Com funciona aquesta anàlisi 35

09 Estat del CMS **37**

10 Versió i suport de PHP **44**

11 Integritat del nucli de WordPress **46**

12 Exposició i superfície d'atac **48**

13 Directives malicioses de configuració **50**

14 Atacs detectats als registres **52**

15 Trànsit i indicadors de xarxa maliciosos **56**

16 Risc per pais de l'origen del trafic **59**

17 Matriu d'Impacte al Negoci **62**

18 Conclusions **64**

Anàlisi de SWPANEL.COM generat per SWPanel

01

Resum executiu de seguretat

Visió de conjunt de l'estat de seguretat del lloc i les prioritats d'actuació.

Anàlisi de SWPANEL.COM generat per SWPanel

Resum executiu de seguretat

Visió de conjunt de l'estat de seguretat del lloc i les prioritats d'actuació.

PUNTUACIÓ DE RISC

72 / 100

Risc ALT

ACTIVITAT D'ATAC I VULNERABILITATS

9	Atacs contra vulnerabilitats reals de la web
386	Intents d'atac als registres
2	Vulnerabilitats conegudes (CVE)
3	IPs malicioses que han accedit
5	Errors de codi

El nivell de risc de la teva web és alt, amb un score de 72 sobre 100, principalment perquè s'han detectat 9 intents d'atac contra vulnerabilitats reals, 386 intents d'intrusió en total i 5 errors de codi que poden obrir camins inesperats. Aquestes dades indiquen que la teva web és un objectiu concret per part d'atacants que intenten aprofitar-se de falles conegudes i no resoltes. Tot i això, no hi ha cap rastre de codi maliciós al disc ni cap connexió amb una infraestructura de control externa, per tant, no hi ha indicis que algú hagi pogut accedir al sistema de forma activa. Això no vol dir que no hi hagi risc, sinó que, per ara, no hi ha senyals que l'atac hagi pogut tenir èxit.

El que cal tenir en compte és que els 9 intents d'atac contra vulnerabilitats reals són molt més greus que els 386 intents generals, perquè aquests últims són com a cops a la porta que fan els atacants cada dia i que, per si sols, no volen dir que hi hagi intrusió. En canvi, els 9 intents contra vulnerabilitats reals són com a claus que ja saben que poden obrir una porta si no està tancada. A més, hi ha 2 vulnerabilitats conegudes (CVE) sense resoldre, amb una puntuació de risc moderat (CVSS màxim 5.4), i 5 errors de codi que poden complicar la seguretat. Tot això suma, però no vol dir que la web sigui insegura per defecte.

El que ja està sota control és que no hi ha cap senyal de compromís actual, i el gestor de continguts (WordPress 6.8.2) encara està en suport. El que pesa de veritat són els falles que ja es poden aprofitar, i que cal tancar aviat. El risc no és imminent, però no es pot ignorar. Si es resolen les prioritats, es pot reduir molt la superfície d'atac i tranquil·litzar la situació.

PRIORITATS

Anàlisi de SWPANEL.COM generat per SWPanel

Resum executiu de seguretat

1. Tancar les 2 vulnerabilitats conegudes (CVE) que no tenen exploit públic però que poden ser explotades si no es resolen — URGENT
2. Revisar i corregir els 5 errors de codi que poden afectar la seguretat
3. Revisar els 2 errors SQL que poden permetre accés no autoritzat a dades

CONTEXT

És important entendre que molts dels 386 intents d'atac són part del ruido habitual d'internet, com a programes automàtics que intenten accedir a qualsevol web. Aquests no volen dir que la teva web sigui especialment vulnerable, sinó que és una realitat del món digital. El que sí cal atendre són els 9 intents contra vulnerabilitats reals, perquè aquests són casos concrets on un atacant sap que hi ha una porta oberta.

Tot i això, la situació no és desesperada. El fet que no hi hagi codi maliciós ni connexions amb servidors maliciosos vol dir que, per ara, no hi ha intrusió activa. El que cal fer és tancar les portes que ja es poden obrir, perquè un atac no espera que tu ho resolguis. Si es resolen les prioritats, es pot reduir molt la superfície d'atac i tranquil·litzar la situació.

FULL DE RUTA

1. Fer un audit complet de les 2 CVE i corregir-les immediatament — URGENT
2. Revisar i corregir els 5 errors de codi i els 2 errors SQL a les properes setmanes
3. Establir un pla de revisió periòdica de la seguretat per mantenir el sistema actualitzat i protegit

Anàlisi de SWPANEL.COM generat per SWPanel

02

Resum de l’anàlisi

Errors de codi detectats als logs d'Apache/Nginx, la seva gravetat i els fitxers afectats.

Anàlisi de SWPANEL.COM generat per SWPanel

Introducció

Aquesta eina analitza automàticament els logs del servidor web per localitzar errors de programació reals que estan passant en producció i proposar-ne la correcció. No és una anàlisi teòrica: treballa sobre els errors que les visites estan provocant ara mateix.

Es revisen els logs de les diferents capes del servidor web: els logs proporcionats. Cada petició que falla per un error de codi deixa un rastre en aquests logs, amb el fitxer i la línia exactes on s'ha produït.

Què busquem: només errors de programació que es puguin corregir, és a dir, els que apunten a un fitxer de codi concret i a una línia. Els accessos normals, els 404 i els problemes d'infraestructura (timeouts, upstreams) es descarten automàticament.

Patrons detectats: errors de PHP (Parse, Fatal, Warning, Notice, Deprecated, Recoverable i excepcions Uncaught) i, en general, qualsevol error amb una referència clara a un fitxer i una línia (on line N o fitxer:N), tant a Apache com a Nginx.

Com treballa: descarrega els logs, els analitza línia a línia, agrupa els errors per fitxer afectat i, per a cada fitxer, el Motor IA de SWPanel, entrenat i especialitzat en codi, proposa el diagnòstic de la causa arrel i el fitxer ja corregit, a punt per revisar i aplicar.

Anàlisi de SWPANEL.COM generat per SWPanel

Resum executiu

Síntesi de l'estat del codi segons els errors capturats als logs d'Apache/Nginx.

SITUACIÓ

5	5	Tema + plugins
errors únics	patrons diferents	components afectats

Errors repetits que afecten components clau del sistema i poden provocar errors en la visualització o el funcionament de determinades seccions del lloc.

ERRORS DETECTATS · PER PRIORITAT DE CORRECCIÓ

PRIORITAT

1

Type error tema - template-tags.php

Uncaught TypeError: count(): Argument #1 ($value) must be of type Countable|array, null given

› **Acció:** corregir el tipus de dada passat a la funció; pot afectar la generació de feeds i la indexació del lloc.

PRIORITAT

2

Memoria esgotada plugin - export.php

PHP Fatal error: Allowed memory size of 268435456 bytes exhausted (tried to allocate 20480 bytes)

› **Acció:** revisar i corregir el codi afectat per evitar el problema.

PRIORITAT

3

Acces a propietats nul-les tema - functions.php

Warning: Attempt to read property "post_title" on null

› **Acció:** verificar i corregir per evitar errors en la visualització de continguts.

Anàlisi de SWPANEL.COM generat per SWPanel

Errors detectats

Llista d'errors únics detectats (les repeticions s'agrupen). Ordenats tal com apareixen al log.

	Tipus	Fitxer	Lín	Missatge
1	Type error ×37	...theme/inc/template-tags.php	142	Uncaught TypeError: count(): Argument #1 ($value) must be of type Countable|array, null gi
2	Acces a propietats nul-les ×12	...swpanel-theme/functions.php	88	Warning: Attempt to read property "post_title" on null
3	Clau d'array inexistent ×214	.../includes/class-pricing.php	56	Warning: Undefined array key "currency"
4	Deprecated ×1480	.../includes/class-pricing.php	23	Deprecated: Creation of dynamic property SW_Pricing::$plans is deprecated
5	Memoria esgotada ×3	...ontact-forms/lib/export.php	301	PHP Fatal error: Allowed memory size of 268435456 bytes exhausted (tried to allocate 20480

Anàlisi de SWPANEL.COM generat per SWPanel

03

Seguretat i detecció de programari maliciós

Patrons maliciosos, ofuscació, backdoors i signes de compromís detectats al codi.

Anàlisi de SWPANEL.COM generat per SWPanel

Seguretat i detecció de programari maliciós

Com analitzem la seguretat del teu codi i com interpretar els resultats.

En aquest capítol revisem el codi dels fitxers implicats buscant senyals de programari maliciós: backdoors, webshells, codi ofuscat (base64, eval), redireccions amagades, spam SEO i altres indicadors que un fitxer ha estat manipulat. L'anàlisi combina dos passos: un escàner que busca patrons coneguts de programari maliciós i una avaluació feta pel Motor IA de SWPanel, entrenat i especialitzat en codi.

Per a cada fitxer mostrem els indicadors detectats (amb la seva línia i una descripció) i un veredicte —net, sospitós o compromès— acompanyat del seu raonament. Les conclusions es basen en aquests indicadors i en el context del codi, no en suposicions. Això t'ajuda a saber quins fitxers mereixen una revisió prioritària i per què, abans de tocar res.

UNA NOTA IMPORTANT SOBRE EL MOTOR IA DE SWPANEL

Aquesta avaluació la genera el Motor IA de SWPanel, el nostre motor intel·ligent entrenat i especialitzat en codi. Com qualsevol motor d'aquest tipus, pot equivocar-se: tant marcar com a sospitós codi legítim com passar per alt una amenaça real. Pren-la com una opinió orientativa, no com un veredicte definitiu. Abans d'esborrar o modificar cap fitxer, contrasta les seves conclusions amb un professional o expert en desenvolupament web.

Anàlisi de SWPANEL.COM generat per SWPanel

Seguretat i detecció de programari maliciós

`/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php`

Veredicte: NET - cap indici de compromís

Motor IA de SWPanel

El fitxer ha superat l'anàlisi de seguretat sense detectar codi maliciós ni manipulació.

INDICADORS DE L'AVALUACIÓ

No hi ha eval. base64 ofuscat, webshells ni crides a system()/exec().

- webshell
- eval
- base64 ofuscat
- injeccions
- execució remota

El codi coincideix amb l'estructura habitual d'un tema/plugin de WordPress.

RECOMANACIÓ

SEGUIMENT RECOMANAT

`inc/template-tags.php`

Aplicar la correcció proposada i mantenir el fitxer sota control de versions.

Anàlisi de SWPANEL.COM generat per SWPanel

Seguretat i detecció de programari maliciós

`/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php`

Veredicte: NET - cap indici de compromís

Motor IA de SWPanel

El fitxer ha superat l'anàlisi de seguretat sense detectar codi maliciós ni manipulació.

INDICADORS DE L'AVALUACIÓ

No hi ha eval. base64 ofuscat, webshells ni crides a system()/exec().

- webshell
- eval
- base64 ofuscat
- injeccions
- execució remota

El codi coincideix amb l'estructura habitual d'un tema/plugin de WordPress.

RECOMANACIÓ

SEGUIMENT RECOMANAT

`swpanel-theme/functions.php`

Aplicar la correcció proposada i mantenir el fitxer sota control de versions.

Anàlisi de SWPANEL.COM generat per SWPanel

Seguretat i detecció de programari maliciós

`/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.ph`

Veredicte: NET - cap indici de compromís

Motor IA de SWPanel

El fitxer ha superat l'anàlisi de seguretat sense detectar codi maliciós ni manipulació.

INDICADORS DE L'AVALUACIÓ

No hi ha eval. base64 ofuscat, webshells ni crides a system()/exec().

- webshell
- eval
- base64 ofuscat
- injeccions
- execució remota

El codi coincideix amb l'estructura habitual d'un tema/plugin de WordPress.

RECOMANACIÓ

SEGUIMENT RECOMANAT

`includes/class-pricing.php`

Aplicar la correcció proposada i mantenir el fitxer sota control de versions.

Anàlisi de SWPANEL.COM generat per SWPanel

Seguretat i detecció de programari maliciós

`/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php`

Veredicte: SOSPITÓS - requereix revisió manual

S'han detectat patrons que requereixen una revisió manual del fitxer.

Motor IA de SWPanel

Indicadors detectats

Severitat	Patró	Lín	Descripció
ALT	unserialize($_POST)	118	Deserialitza dades enviades per l'usuari: pot permetre injecció d'objectes PHP.

INDICADORS DE L'AVALUACIÓ

unserialize() sobre $_POST['filters'] a la línia 118: un atacant podria injectar objectes PHP.

No hi ha indicis de codi maliciós: és un error de disseny, no una infecció.

RECOMANACIÓ

SEGUIMENT RECOMANAT

`lib/export.php`

Substituir unserialize() per json_decode() i validar els camps rebuts.

Anàlisi de SWPANEL.COM generat per SWPanel

04

Correccions proposades

Diagnòstic de la causa arrel i codi corregit, fitxer a fitxer, generat pel Motor IA de SWPanel.

Anàlisi de SWPANEL.COM generat per SWPanel

Fitxer 1 de 4

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php

Llenguatge: php Errors: 1

CORRECCIÓ PROPOSADA

```
Type error (línia 142): Uncaught TypeError: count(): Argument #1 ($value) must be of type
Countable|array, null given
```

DIAGNÒSTIC

A la línia 142 es crida count() sobre el resultat de get_the_category(). Quan una entrada no té categories (esborranys importats o pàgines de producte), la funció retorna null i PHP 8 llança un TypeError que talla el llistat del blog.

CANVIS

LÍNIES 142	Es força un array buit quan no hi ha categories abans de comptar-les.

RISC

Baix: només canvia el cas sense categories, que avui falla.

» Veure el **Codi corregit** a la pàgina següent.

Anàlisi de SWPANEL.COM generat per SWPanel

Codi corregit

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/inc/template-tags.php

</> template-tags.php — codi actual — correcció proposada

```
1  1  $cats = get_the_category( $post_id );
-  2+ if ( ! is_array( $cats ) ) {
-  3+     $cats = array();
-  4+ }
2  5  if ( count( $cats ) > 1 ) {
3  6      echo '<span class="cat-list">' . esc_html( $cats[0]->name ) . '</span>';
4  7  }
```

Anàlisi de SWPANEL.COM generat per SWPanel

Fitxer 2 de 4

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php

Llenguatge: php Errors: 1

CORRECCIÓ PROPOSADA

```
Acces a propietats nul-les (línia 88): Warning: Attempt to read property "post_title" on null
```

DIAGNÒSTIC

get_post() retorna null quan l'ID de la pàgina destacada configurada al personalitzador ja no existeix; després es llegeix ->post_title sense comprovar-ho.

CANVIS

LÍNIES 88	Es comprova que l'entrada existeixi abans d'usar-ne el títol.

RISC

Baix.

» Veure el **Codi corregit** a la pàgina següent.

Anàlisi de SWPANEL.COM generat per SWPanel

Codi corregit

/var/www/swpanel.com/datos/web/wp-content/themes/swpanel-theme/functions.php

</> functions.php — codi actual — correcció proposada

```
1  1  $featured = get_post( get_theme_mod( 'sw_featured_page' ) );
2  -  $title = $featured->post_title;
-  2  $title = $featured instanceof WP_Post ? $featured->post_title : '';
```

Anàlisi de SWPANEL.COM generat per SWPanel

Fitxer 3 de 4

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.php

Llenguatge: php Errors: 2

CORRECCIÓ PROPOSADA

```
Clau d'array inexistent (línia 56): Warning: Undefined array key "currency" Deprecated (línia 23): Deprecated: Creation of dynamic property SW_Pricing::$plans is deprecated
```

DIAGNÒSTIC

La classe SW_Pricing crea la propietat $plans sense declarar-la (obsoleta des de PHP 8.2) i llegeix $opts['currency'] sense valor per defecte quan el pla no té moneda.

CANVIS

LÍNIES 56, 23	Es declara la propietat i s'usa EUR per defecte.

RISC

Nul: no canvia el comportament visible.

» Veure el **Codi corregit** a la pàgina següent.

Anàlisi de SWPANEL.COM generat per SWPanel

Codi corregit

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-pricing-table/includes/class-pricing.php

</> class-pricing.php — codi actual — correcció proposada

```
 1  1  class SW_Pricing {
 -  2+     public array $plans = array();
 -  3+     public string $currency = 'EUR';
 2  4      public function __construct( $opts ) {
 3  -          $this->plans = $opts['plans'];
 4  -          $this->currency = $opts['currency'];
 -  5+         $this->plans = $opts['plans'] ?? array();
 -  6+         $this->currency = $opts['currency'] ?? 'EUR';
```

Anàlisi de SWPANEL.COM generat per SWPanel

Fitxer 4 de 4

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php

Llenguatge: php Errors: 1

CORRECCIÓ PROPOSADA

```
Memoria esgotada (línia 301): PHP Fatal error: Allowed memory size of 268435456 bytes
exhausted (tried to allocate 20480 bytes)
```

DIAGNÒSTIC

L'exportació carrega tots els enviaments del formulari a memòria d'un sol cop (uns 61.000) abans d'escriure el CSV i supera el límit de 256 MB.

CANVIS

LÍNIES 301	Es llegeix per lots de 500 registres i s'escriu el CSV a mesura.

RISC

⚠ Baix: provar una exportació completa després d'aplicar-ho.

» Veure el **Codi corregit** a la pàgina següent.

Anàlisi de SWPANEL.COM generat per SWPanel

Codi corregit

/var/www/swpanel.com/datos/web/wp-content/plugins/sw-contact-forms/lib/export.php

</> export.php — codi actual — correcció proposada

```
- $rows = $wpdb->get_results( "SELECT * FROM {$table}" );
- foreach ( $rows as $r ) {
-     fputcsv( $out, (array) $r );
- }
+ $offset = 0;
+ do {
+     $rows = $wpdb->get_results( $wpdb->prepare( "SELECT * FROM {$table} LIMIT %d, 500"
+     foreach ( $rows as $r ) {
+         fputcsv( $out, (array) $r );
+     }
+     $offset += 500;
+ } while ( count( $rows ) === 500 );
```

Anàlisi de SWPANEL.COM generat per SWPanel

05

Errors SQL detectats

Sentències SQL que han fallat segons els logs, amb la correcció suggerida.

Anàlisi de SWPANEL.COM generat per SWPanel

Errors SQL detectats

Sentències SQL que han fallat segons els logs, amb la correcció suggerida.

• Permisos / connexió BBDD • Fals positiu · log truncat • Correcció proposada

Error SQL 1 ×642

PERMISOS / CONNEXIÓ BBDD

642 ocurrències al log

```
WordPress database error Unknown column 'plan_slug' in 'where clause' for query SELECT * FROM wp_sw_pricing WHERE plan_slug = 'cloud-pro'
```

CONSULTA DETECTADA

```
SELECT * FROM wp_sw_pricing WHERE plan_slug = 'cloud-pro'
```

La columna es va reanomenar a 'slug' a la versió 2.0 del plugin, però aquesta consulta encara usa el nom antic.

CORRECCIÓ PROPOSADA

Concedir permisos d'escriptura a l'usuari de BBDD (o revisar la configuració de connexió a wp-config.php).

```
SELECT * FROM wp_sw_pricing WHERE slug = 'cloud-pro'
```

Error SQL 2 ×9

PERMISOS / CONNEXIÓ BBDD

9 ocurrències al log

```
WordPress database error Deadlock found when trying to get lock; try restarting transaction for query UPDATE wp_options SET option_value = '...' WHERE option_name = '_transient_sw_rates'
```

CONSULTA DETECTADA

```
UPDATE wp_options SET option_value = '...' WHERE option_name = '_transient_sw_rates'
```

La consulta és correcta: dos processos de wp-cron actualitzen el mateix transient alhora. Convé desactivar wp-cron per visita i llançar-lo des d'un cron del sistema.

CORRECCIÓ PROPOSADA

Concedir permisos d'escriptura a l'usuari de BBDD (o revisar la configuració de connexió a wp-config.php).

Anàlisi de SWPANEL.COM generat per SWPanel

06

Diagnòstic del trànsit

Explicació en llenguatge planer del que mostren els logs i accions recomanades.

Anàlisi de SWPANEL.COM generat per SWPanel

Diagnòstic del trànsit

A partir del que mostren els logs, aquí tens el resum en llenguatge clar i les accions recomanades.

Gravetat: ALTA

El lloc web està exposat a múltiples intents de violació, atacs de força bruta i rastrejos agressius, amb risc real de compromís de dades o vulnerabilitat. ###DIAGNOSTIC### - S'han detectat 23 intents de injecció SQL i XSS, com ara l'ús de codi maliciós per accedir a dades d'usuari. - Hi ha 1.312 intents de rastreig agressiu, on bots busquen fitxers sensibles com `.env` o `wp-config.php.bak`. - S'han registrat 418 intents de força bruta a les pàgines de login, especialment a `/wp-login.php` i `/xmlrpc.php`. - El lloc ha rebut 2.870 pàgines no trobades (404), la majoria des de IPs ja identificades com a sospitoses. - El lloc ha rebut 356 accés denegats (403), sovint a fitxers clau de WordPress com `.htaccess` o `wlwmanifest.xml`.

QUÈ ESTÀ PASSANT

Intents d'entrar per força

Algú prova contrasenyes repetidament per colar-se al lloc. 418 intents detectats. Sobretot des de 203.0.113.77.

Escaneig buscant forats

Proven d'obrir fitxers de configuració sensibles per trobar punts febles. 1312 peticions.

Intents d'injecció

Peticions amb codi maliciós (SQL/XSS) per manipular la web. 23 casos.

Intents d'obrir fitxers prohibits

403

Intents d'accés a fitxers ocults o sensibles. El servidor els ha bloquejat.

Cerca de pàgines inexistents

404

Peticions a pàgines que no existeixen, sovint per sondejar el lloc. 2870 casos.

Errors interns del servidor

500

El servidor ha tingut problemes per respondre, potser per sobrecàrrega. 41 errors.

La infraestructura aguanta

Sense timeouts ni errors de connexió entre Nginx i Apache. La infraestructura funciona.

Anàlisi de SWPANEL.COM generat per SWPanel

Diagnòstic del trànsit

QUÈ CAL FER

1. **Activa la CDN de Cloudflare al SWPanel** per protegir el lloc d'atacs externs. Aquesta funció filtra bots, IPs malicioses i atacs abans que arribin al servidor. URGENT

2. **Utilitza el Fail2Ban gestionat** per bloquejar automàticament IPs que intentin accedir repetidament a pàgines de login.

3. **Bloqueja manualment les IPs més actives d'atac** (203.0.113.45, 198.51.100.23, 203.0.113.77, 192.0.2.150) amb iptables si no pots fer-ho des del SWPanel.

```
iptables -A INPUT -s 203.0.113.45 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 192.0.2.150 -j DROP
```

4. **Revisa la configuració de WordPress** per assegurar-te que fitxers com .env, .git o wp-config.php.bak no siguin accessibles des del navegador.

5. **Actualitza totes les extensions i temes de WordPress** per garantir que no hi hagi vulnerabilitats conegudes.

Anàlisi de SWPANEL.COM generat per SWPanel

IP a bloquejar

No cal que toquis res tècnic

Aquestes són les 5 IP malicioses que cal bloquejar. La manera més senzilla és fer-ho des del teu SWPanel amb un parell de clics, sense comandes ni accés al servidor. Si ho prefereixes, més avall tens les comandes exactes per al teu tècnic.

LA MANERA MÉS SENZILLA: ACTIVA LA CDN DE CLOUDFLARE

CDN de Cloudflare

RECOMANAT

Aquest servei no està dins d'un Cloud, així que el FW de Capa 4 no hi és disponible. Activa la CDN de Cloudflare des del teu SWPanel: fa de proxy i filtra el trànsit maliciós (IP, països i bots) abans que arribi al teu lloc, sense comandes ni accés al servidor.

IP A BLOQUEJAR

- `203.0.113.77`
- `192.0.2.150`
- `203.0.113.45`
- `198.51.100.23`
- `198.51.100.88`

ALTERNATIVA MANUAL PER AL TEU TÈCNIC: COMANDES IPTABLES

```
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 192.0.2.150 -j DROP
iptables -A INPUT -s 203.0.113.45 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
iptables -A INPUT -s 198.51.100.88 -j DROP
```

Cada línia bloqueja una IP. Demana al teu tècnic que les apliqui i les faci permanents (perquè no es perdin en reiniciar). I com que ja tens el Fail2Ban Gestionat actiu, configura'l a Seguretat > Fail2Ban perquè bloquegi automàticament els futurs atacants.

Anàlisi de SWPANEL.COM generat per SWPanel

07

Trànsit i seguretat (logs d’accés)

Troballes detectades analitzant els logs d'accés del servidor web.

Anàlisi de SWPANEL.COM generat per SWPanel

Trànsit i seguretat (logs d'accés)

Troballes detectades analitzant els logs d'accés del servidor web. (186420 peticions analitzades)

Severitat	Categoria	Nº	Mostra
CRÍTIC	Injecció a la URL	23	
ALT	Escaneig de fitxers sensibles	1.312	
ALT	Intents d'accés / força bruta	418	
ALT	Errors de servidor (5xx)	41	
MITJÀ	Accessos bloquejats (reconeixement)	356	
MITJÀ	Pàgines no trobades (404)	2.870	

Detall dels accessos detectats

CRÍTIC

Injecció a la URL

23 peticions

RUTES PRINCIPALS	ORIGEN (IPS IMPLICADES)	REPETICIONS
`/?s=%27+union+select+user_login,user_pass`	`198.51.100.23`	17
`/?p=1%3Cscript%3Ealert(1)%3C/script%3E`	`203.0.113.45`	6

ALT

Escaneig de fitxers sensibles

1.312 peticions

RUTES PRINCIPALS	ORIGEN (IPS IMPLICADES)	REPETICIONS
`/.env`	`203.0.113.45`	610
`/wp-config.php.bak`	`198.51.100.23`	402
`/.git/config`		
`/phpinfo.php`		

Anàlisi de SWPANEL.COM generat per SWPanel

Trànsit i seguretat (logs d'accés)

Detall dels accessos detectats (continuació)

ALT

Intents d'accés / força bruta

418 peticions

RUTES PRINCIPALS	ORIGEN (IPS IMPLICADES)	REPETICIONS
`POST /wp-login.php`	`203.0.113.77`	296
`POST /xmlrpc.php`	`192.0.2.150`	122

Errors de servidor (5xx) 41

`500 /blog/`
`500 /wp-admin/admin-post.ph`

Pàgines no trobades (404) 2.870

`/precios-antiguos/`
`/wp-content/uploads/2024/03/`

IP principal: 203.0.113.45 (940)

Accessos bloquejats (reconeixement) 356

`/wp-content/uploads/.htacces`
`/wp-includes/wlwmanifest.xml`

PATRONS DETECTATS A LES MOSTRES (OWASP CRS)

- Injecció SQL (SQLi): 2
- Execució de codi (RCE): 8

Recomanacions prioritàries

CRÍTIC

Injecció a la URL

aquests intents busquen executar SQL o llegir fitxers del sistema. Revisa que totes les entrades es validen i que s'usen consultes parametritzades, i considera afegir regles de WAF.

ALT

Escaneig de fitxers sensibles

bloqueja l'accés a rutes com .env, .git, wp-config i phpMyAdmin des del servidor web o el WAF i comprova que aquests fitxers no són accessibles públicament.

ALT

Intents d'accés / força bruta

limita els intents d'inici de sessió, activa l'autenticació en dos passos a wp-login i al panell d'administració, i bloqueja les IPs reincidents (fail2ban o WAF).

ALT

Errors de servidor (5xx)

indiquen errors del backend o de l'aplicació en producció. Revisa els logs d'error de les rutes afectades i corregeix-ne la causa per no perdre peticions legítimes.

Anàlisi de SWPANEL.COM generat per SWPanel

Trànsit i seguretat (logs d'accés)

Recomanacions prioritàries

MITJÀ

Pàgines no trobades (404)
un volum alt pot indicar enllaços trencats o contingut eliminat. Revisa les URLs més freqüents i afegeix redireccions 301 cap al destí correcte.

Anàlisi de SWPANEL.COM generat per SWPanel

08

Errors de JavaScript

Errors reals detectats en carregar les teves pàgines en un navegador, amb el codi que falla i la seva correcció.

Anàlisi de SWPANEL.COM generat per SWPanel

Errors de JavaScript

Com analitzem el JavaScript del teu web i com llegir els resultats.

Per a aquesta anàlisi carreguem les teves pàgines en un navegador real (Chromium, sense finestra) i registrem què passa: errors a la consola, excepcions de JavaScript i recursos que no carreguen. Revisem diverses pàgines del domini, preses dels registres d'accés (les més visitades) i del sitemap.xml.

Per a cada error mostrem en quina pàgina passa, el fitxer i la línia, i si és codi teu (primera part) o d'un servei extern (tercers). Quan és codi teu, mostrem el fragment que falla i una correcció proposada. També identifiquem les llibreries de mercat que fas servir i quants scripts carrega cada pàgina, perquè un excés de scripts alenteix el web.

UNA NOTA IMPORTANT SOBRE EL MOTOR IA DE SWPANEL

L'anàlisi i les correccions d'aquest capítol les genera el Motor IA de SWPanel, entrenat i especialitzat en codi, sobre el que captura un navegador real. Com qualsevol motor d'aquest tipus, pot equivocar-se o proposar un canvi que no encaixi amb el teu codi. Pren-ho com una orientació: abans d'aplicar cap correcció, prova-la i contrasta-la amb un professional o expert en desenvolupament web.

Anàlisi de SWPANEL.COM generat per SWPanel

Errors de JavaScript

18 pàgines analitzades en un navegador real.

Errors al teu codi (primera part)

TypeError (codi teu) ×17

Pàgina: https://swpanel.com/precios/ · https://swpanel.com/wp-content/themes/swpanel-theme/js/pricing-toggle.js

Uncaught TypeError: Cannot read properties of null (reading 'addEventListener')

CODI AMB ERROR

```
document.querySelector('#billing-switch').addEventListener('change', onToggle);
```

CORRECCIÓ PROPOSADA

```
const sw = document.querySelector('#billing-switch');.if (sw) { sw.addEventListener('change', onToggle); }
```

Explicació: L'script es carrega a totes les pàgines, però l'interruptor mensual/anual només existeix a /precios/.

Llibreries de JavaScript detectades

jQuery
3.7.1

Swiper
8.4.7

Càrrega de scripts per pàgina

Nombre de scripts que carrega cada pàgina. Massa scripts —o molt pesats— alenteixen la càrrega i empitjoren l'experiència.

Pàgina	Externs	En línia	Total	Estat
/	24	11	**35**	Massa scripts
/precios/	27	13	**40**	Massa scripts

Anàlisi de SWPANEL.COM generat per SWPanel

09

Estat del CMS

Gestor de continguts detectat, la seva versió i si està actualitzat, desactualitzat o sense suport.

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

Detectem el gestor de continguts (CMS) del teu web i la seva versió llegint-los directament al servidor, i els comparem amb la darrera versió oficial i amb la data de fi de suport (EOL). Un CMS sense suport ja no rep pegats de seguretat i és un risc.

Versió del gestor

ON ETS · INSTAL·LADA

6.8.2

ON CAL ANAR · RECOMANADA

6.8.3

• Amb suport

Gestor de continguts: WordPress Fi de suport (EOL): -

Vulnerabilitats conegudes (CVE)

S'han detectat 1 vulnerabilitats (CVE) públiques que afecten la versió instal·lada. CVSS màxim: 5.4 (MEDIUM). Exemples: CVE-2026-0000 (5.4). EPSS max: 0%. Mostra recent dels CVE més nous; la cobertura completa requereix el mòdul de vulnerabilitats en cache.

Vulnerabilitats conegudes de plugins i temes

1 plugins/temes amb vulnerabilitats conegudes (1 CVE en total). Puntuacio maxima: 6.4 (MEDIUM). Components afectats: contact-form-7 5.9.8 (1 CVE, max 6.4). EPSS max: 0%. Actualitza els plugins i temes a la darrera versio disponible.

Plugins i temes desactualitzats

2

• 2 amb salt de versió major (prioritaris) • 0 amb salt menor Total: 2

Component	Tipus	Instal·lada	Darrera	Salt
PRIORITARIS · SALT DE VERSIÓ MAJOR				
Contact Form 7	PLUGIN	5.9.8	6.1.1	MAJOR
Yoast SEO	PLUGIN	25.4	26.1	MAJOR

QUÈ SIGNIFICA I QUÈ CAL FER

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

El gestor de continguts del seu lloc web és WordPress, i la versió instal·lada és la 6.8.2, que ja no és la més recent. Això vol dir que hi ha una versió més nova disponible, la 6.8.3, que és la recomanada per mantenir el sistema segur i actualitzat. Un gestor de continguts desactualitzat és com una porta d'entrada a casa que ja no tingués el reforç més recent: pot tenir agujeros que no es coneguin encara, però que poden aparèixer i no tindran solució fins que s'actualitzi. Si no es passa a la versió més nova, aquests problemes poden anar acumulant-se i fer-se més difícils i costosos de resoldre amb el temps.

El seu gestor actual té 2 vulnerabilitats conegudes i documentades. Aquestes són falles de seguretat que ja han estat identificades i publicades, però que encara no tenen cap codi d'atac públic disponible, per tant no són fàcils d'aprofitar. Cap d'aquestes vulnerabilitats està sent actualment explotada en atacs reals, i la més greu té un nivell de gravetat de 6.4 sobre 10, que és moderadament greu. Això vol dir que, si algú decidís atacar el seu lloc web, podria aprofitar aquestes falles per introduir-se, robar dades, inyectar contingut no desitjat o fins i tot fer caure el lloc, cosa que afectaria la seva reputació i la continuïtat del seu servei.

Per resoldre això, la millor opció és actualitzar el gestor de continguts a la versió recomanada, la 6.8.3. Aquesta actualització és normalment senzilla i no sol causar problemes si s'ha mantingut el sistema fins ara. Si cal, es pot fer una prova prèvia per assegurar que tot funciona com cal. Mantenir el gestor actualitzat és una de les defenses més eficaces i econòmiques que existeixen, perquè tanca la majoria d'aquestes portes obertes sense gaires complicacions. Si no s'actualitza, aquestes falles poden anar creixent i acabar sent més difícils de gestionar.

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

Full de ruta d'actualització

La teva situació

La teva versió 6.8.2 es va publicar fa un any. La versió actual és la 7.0 (maig 2026).

EN POQUES PARAULES

Actualitzar el gestor de continguts del seu lloc web és una inversió clara en la seva seguretat i funcionalitat. Si el seu CMS ja té un any d'antiguitat, encara és relativament recent, però cada dia que passa sense actualitzar s'exposa més a riscos que poden ser difícils de gestionar més endavant. Si el seu sistema ja no té suport, o si ha estat molt de temps sense actualitzar, pot haver-hi més passos intermedis per fer i més atenció a detalls, però això no vol dir que sigui impossible. Al contrari: si s'avança pas a pas i amb calma, el camí és del tot recorrible i el resultat val la pena.

El mètode més segur implica començar amb una bona còpia de seguretat, que cal assegurar-se que es pot restaurar de debò. Després, es fa una prova en un entorn separat, com una còpia del lloc, per veure com funciona l'actualització abans de fer-la en el lloc real. Si cal, s'avança per etapes, sense saltar versions si això pot causar problemes. També és important revisar que tots els plugins, mòduls i dissenys que utilitza encara funcionin bé després de l'actualització. Si el canvi és més gran del que s'espera, no hi ha cap problema a buscar ajuda professional. El que sí és clar és que mantenir el gestor actualitzat és la millor manera de protegir el seu lloc web i garantir que segueixi funcionant bé al llarg del temps.

VERSIONS I DATES

- **6.8.2** abr 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — LA TEVA VERSIÓ
- **6.9** des 2025 — PHP 7.2+ · MySQL 5.7+ / MariaDB 10.4+ — PAS INTERMEDI
- **7.0** maig 2026 — PHP 7.4+ · MySQL 8.0+ / MariaDB 10.6+ — VERSIÓ ACTUAL

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

QUÈ NECESSITA LA VERSIÓ DESTÍ

PHP	Necessites PHP 8.3 o superior (el minim absolut es 7.4, pero ja esta sense suport). L'ideal es 8.4.
Base de dades	MySQL 8.0 o superior, o be MariaDB 10.6 o superior (recomanat).
Memòria / RAM	El fabricant no publica un minim de RAM oficial.
Altres requisits	HTTPS obligatori. Servidor Apache 2.4 o Nginx 1.26 o superior.

Requisits segons la documentació oficial del fabricant: https://wordpress.org/about/requirements/

PASSOS RECOMANATS

1

Fes una copia de seguretat completa i comprova que es pot restaurar

Abans de tocar res, guarda una copia de tot el lloc: els fitxers (tema, plugins i la carpeta de pujades) i tambe la base de dades, que es on hi ha els textos i la configuracio. Pots fer-ho des del panell del teu allotjament (sovint hi ha un boto Copia de seguretat) o demanant-ho al suport del proveidor; si tens un plugin de copies, llanca una copia completa i descarrega-la al teu ordinador. El mes important es comprovar que la copia es pot restaurar de veritat: si pots, recupera-la en una copia de proves abans de continuar.

Guia oficial de copies de seguretat
https://developer.wordpress.org/advanced-administration/security/backup/

2

Posa al dia el servidor: PHP 8.3 o superior i la base de dades recomanada

WordPress 7.0 demana un servidor modern: PHP 8.3 o superior i la base de dades a MariaDB 10.6 o superior, o be MySQL 8.0 o superior. No has de tocar codi: aquests canvis es fan des del panell del teu allotjament, en una seccio com Versio de PHP, o demanant-ho al suport del proveidor. Comprova quina versio tens ara i, si va endarrerida, demana que la pugin a la recomanada. Evita quedar-te en versions antigues de PHP marcades com a fora de servei, perque son un risc de seguretat.

Requisits oficials de WordPress
https://wordpress.org/about/requirements/

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

3

Prova primer en un entorn de proves i revisa tema i plugins

No facis l'actualitzacio directament sobre el lloc real: fes una copia de proves (molts allotjaments tenen un boto Staging) i actualitza alli primer. En aquesta copia, desactiva temporalment els plugins i comprova si el tema i cada plugin son compatibles amb la nova versio: a Plugins, dins l'administrador, veuras avisos de tipus Compatible o No provat amb la teva versio. Revisa especialment els plugins antics o que ja no reben actualitzacions, que son els que solen donar problemes.

Provar WordPress en proves
https://developer.wordpress.org/advanced-administration/debug/test-driving/

4

Actualitza el nucli de WordPress, millor per etapes si vas molt endarrerit

Un cop fet el pas de proves, actualitza el nucli entrant a l'administrador i anant a Tauler -> Actualitzacions, on trobaras el boto Actualitza ara. Com que ja tens copia de seguretat pots fer el salt, pero si la teva versio actual es molt antiga es mes segur pujar per etapes (de versio important en versio important) en comptes de fer un sol salt gran. Comprova despres que la pagina principal i l'administrador carreguen be. Evita tancar el navegador mentre s'esta actualitzant.

Guia oficial d'actualitzacio
https://developer.wordpress.org/advanced-administration/upgrade/upgrading/

5

Tanca: actualitza la base de dades, reactiva els plugins i buida la memoria cau

Despres d'actualitzar, si WordPress mostra una pantalla que diu que cal actualitzar la base de dades, fes clic al boto que t'indica per completar-la. Tot seguit torna a Plugins i reactiva un a un els plugins que havies desactivat, comprovant que el lloc segueix funcionant a cada pas. Finalment, buida la memoria cau (al teu plugin de cache o al panell de l'allotjament) perque els visitants vegin la versio nova. Si alguna cosa falla, recorda que tens la copia de seguretat per tornar enrere.

Gestionar i reactivar plugins
https://wordpress.org/documentation/article/manage-plugins/

Compte

A diferencia de la resta, WordPress permet actualitzar directament a l'ultima versio si tens copia de seguretat; tot i aixo, si vas molt endarrerit es mes segur fer-ho per etapes.

Font: https://wordpress.org/documentation/article/updating-wordpress/

Anàlisi de SWPANEL.COM generat per SWPanel

Estat del CMS

Components no verificables (no són al repositori oficial)

3 components

> **No són al repositori oficial**
> No es pot comparar la seva versió amb cap font oficial. Poden ser de pagament o del propi tema (normal), o bé codi afegit sospitós. Revisa al capítol Seguretat els que hi apareguin marcats com a maliciosos.

Component	Tipus	Versió instal·lada
PLUGINS 2		
`sw-pricing-table`	PLUGIN	2.0.3
`sw-contact-forms`	PLUGIN	1.4.0
TEMES 1		
`swpanel-theme`	THEME	3.2.0

> **Recomanació**
> mantén el CMS, els plugins i els temes sempre actualitzats i elimina els que no facis servir. És la manera més eficaç i econòmica de protegir el teu web.

Anàlisi de SWPANEL.COM generat per SWPanel

10

Versió i suport de PHP

La versió de PHP amb què funciona el teu lloc i si encara rep actualitzacions de seguretat.

Anàlisi de SWPANEL.COM generat per SWPanel

Versió i suport de PHP

La versió de PHP amb què funciona el teu lloc i si encara rep actualitzacions de seguretat.

PHP 8.1.31 fora de suport

Aquesta versió de PHP ja no rep actualitzacions de seguretat (fi de suport 31/12/2025). Actualitza a una versió mantinguda des del teu SWPanel per rebre pedaços de seguretat.

display_errors = On

Els errors PHP es mostren al visitant i poden revelar rutes internes. Desactiva-ho en producció.

expose_php = On

La capçalera X-Powered-By anuncia la versió exacta de PHP.

Anàlisi de SWPANEL.COM generat per SWPanel

11

Integritat del nucli de WordPress

Comparem els fitxers principals del nucli de WordPress amb els oficials de wordpress.org (per suma de verificació md5).

Anàlisi de SWPANEL.COM generat per SWPanel

Integritat del nucli de WordPress

Comparem els fitxers principals del nucli de WordPress amb els oficials de wordpress.org (per suma de verificació md5).

El nucli coincideix amb l'oficial

S'han verificat 1284 fitxers clau del nucli; 0 difereixen de l'oficial. No s'ha detectat cap alteració als fitxers verificats.

Anàlisi de SWPANEL.COM generat per SWPanel

12

Exposició i superfície d’atac

Comprovacions actives del domini des de fora: TLS, capçaleres, fitxers exposats i autenticació de correu.

Anàlisi de SWPANEL.COM generat per SWPanel

Exposició i superfície d'atac

Comprovacions actives del domini des de fora: TLS, capçaleres, fitxers exposats i autenticació de correu.

Resum del sondeig
TLS: TLS 1.3. Capçaleres de seguretat: 70/100. Subdominis públics (crt.sh): 3.

Falta Content-Security-Policy
Sense CSP, un script injectat s'executaria sense restriccions.

staging.swpanel.com accessible sense contrasenya
L'entorn de proves és públic i indexable; protegeix-lo amb contrasenya o restricció per IP.

SPF / DKIM / DMARC
SPF i DKIM correctes; DMARC en mode p=none (només informa).

Anàlisi de SWPANEL.COM generat per SWPanel

13

Directives malicioses de configuració

Anàlisi del fitxer .htaccess a l'arrel del lloc: directives que amaguen codi, executen PHP on no toca o exposen carpetes.

Anàlisi de SWPANEL.COM generat per SWPanel

Directives malicioses de configuració

Anàlisi del fitxer .htaccess a l'arrel del lloc: directives que amaguen codi, executen PHP on no toca o exposen carpetes.

Llistat de directoris activat

Options +Indexes exposa el contingut de les carpetes sense índex. Desactiva-ho per no revelar fitxers interns. [Options +Indexes +FollowSymLinks]

Anàlisi de SWPANEL.COM generat per SWPanel

14

Atacs detectats als registres

Peticions als registres d'acces que coincideixen amb vectors d'atac coneguts.

Anàlisi de SWPANEL.COM generat per SWPanel

Atacs detectats als registres

Peticions als registres d'acces que coincideixen amb vectors d'atac coneguts.

Intents d'explotacio detectats
S'han detectat 386 intents d'explotacio de vulnerabilitats conegudes; 9 d'ells van dirigits contra vulnerabilitats que afecten aquesta web.

Els registres del lloc web mostren que ha rebut 386 intents d'atac durant el període analitzat. Aquest tipus de dades són comunes en qualsevol web connectada a internet, ja que els bots maliciosos escanejen constantment en busca de possibles vulnerabilitats. La gran majoria d'aquests intents no tenen èxit perquè no són aplicables a la configuració actual del lloc. No obstant això, és important distingir entre un atac genèric (que no afecta aquest lloc concret) i un atac que explota una vulnerabilitat real del vostre sistema. En aquest cas, 9 dels intents detectats són contra una vulnerabilitat que afecta efectivament el vostre lloc web, i cal atendre'ls amb prioritat.

ATACS DETECTATS

CRÍTIC

9 intents

Contact Form 7 - pujada de fitxer sense validar (CVE-2026-0000)

Aquest atac intenta pujar fitxers maliciosos a través del plugin Contact Form 7, potencialment per instal·lar còdi maliciós. Ha arribat des de l'IP 198.51.100.23, 9 vegades. El vostre lloc web és vulnerable a aquest atac.

ALT

296 intents

Força bruta contra wp-login.php

Aquest atac intenta endevinar credencials d'administrador mitjançant múltiples intents de login. Ha arribat des de l'IP 203.0.113.77, 296 vegades. El vostre lloc web no és vulnerable a aquest atac.

ALT

17 intents

Injecció SQL genèrica (union select)

Aquest atac intenta injectar còdi SQL per accedir a dades sensibles. Ha arribat des de l'IP 198.51.100.23, 17 vegades. El vostre lloc web no és vulnerable a aquest atac.

MITJÀ

64 intents

Lectura de fitxers sensibles (.env / wp-config)

Aquest atac intenta llegir fitxers de configuració per obtenir credencials o claus. Ha arribat des de l'IP 203.0.113.45, 64 vegades. El vostre lloc web no és vulnerable a aquest atac.

Anàlisi de SWPANEL.COM generat per SWPanel

Atacs detectats als registres

IMPLICACIONS

Si l'atac contra el plugin Contact Form 7 tingués èxit, un atacant podria pujar fitxers maliciosos al vostre lloc web, com ara un webshell, que li permetria controlar remotament el sistema. Això podria portar a la pèrdua de control del lloc, la instal·lació de còdi maliciós, o fins i tot al robatori de dades dels usuaris. A més, si aquestes dades inclouen informació personal o sensibles, podria afectar la confiança dels usuaris i generar riscos legals. Els altres intents detectats no afecten directament el vostre lloc web, però és important vigilar-los per si es modifiquen o es tornen aplicables en el futur.

QUÈ CAL FER

1. **Parchear el plugin Contact Form 7** — URGENT

   Aplica immediatament el patch per corregir la vulnerabilitat CVE-2026-0000.

2. **Bloquejar l'IP 198.51.100.23**

   Afegeix aquesta IP a la llista de bloqueig al WAF o a Fail2Ban per evitar més intents.

   ```
   fail2ban-client set sshd banip 198.51.100.23
   ```

3. **Revisar si ja hi ha compromís**

   Revisa els fitxers recents al servidor i el registre d'activitats per detectar qualsevol canvi inusual.

4. **Activar el WAF Adaptatiu**

   Assegura't que el WAF Adaptatiu estigui activat a SWPanel per bloquejar automàticament atacs coneguts.

5. **Monitoritzar i alertar**

   Configura alertes per intents de pujada de fitxers o accés a rutes sensibles, i revisa els logs regularment.

CONTRAMESURES

Contact Form 7 - pujada de fitxer sense validar (CVE-2026-0000):

Anàlisi de SWPANEL.COM generat per SWPanel

Atacs detectats als registres

- **IMMEDIATA:** Aplica el patch de CVE-2026-0000 i bloqueja l'IP 198.51.100.23.

- **TECNICA:** Assegura't que tots els fitxers pujats siguin validats i que només es permetin tipus de fitxer segurs.

- **SWPANEL:** Activa el WAF Adaptatiu a "Seguretat 360" i revisa "Gestió de Hallazgos" per afegir regles específiques.

- **HARDENING:** Mantén tot actualitzat, fes còpies de seguretat regulars i aplica el principi de mínim privilegi als permisos del servidor.

Força bruta contra wp-login.php:

- **IMMEDIATA:** Bloqueja l'IP 203.0.113.77.

- **TECNICA:** No és aplicable a aquest lloc web.

- **SWPANEL:** Activa el WAF Adaptatiu a "Seguretat 360".

- **HARDENING:** Mantén tot actualitzat i fes còpies de seguretat regulars.

Injecció SQL genèrica (union select):

- **IMMEDIATA:** Bloqueja l'IP 198.51.100.23.

- **TECNICA:** No és aplicable a aquest lloc web.

- **SWPANEL:** Activa el WAF Adaptatiu a "Seguretat 360".

- **HARDENING:** Mantén tot actualitzat i fes còpies de seguretat regulars.

Lectura de fitxers sensibles (.env / wp-config):

- **IMMEDIATA:** Bloqueja l'IP 203.0.113.45.

- **TECNICA:** No és aplicable a aquest lloc web.

- **SWPANEL:** Activa el WAF Adaptatiu a "Seguretat 360".

- **HARDENING:** Mantén tot actualitzat i fes còpies de seguretat regulars.

Anàlisi de SWPANEL.COM generat per SWPanel

15

Trànsit i indicadors de xarxa maliciosos

IPs que han accedit a la web i consten en llistes d'infraestructura maliciosa coneguda.

Anàlisi de SWPANEL.COM generat per SWPanel

Trànsit i indicadors de xarxa maliciosos

IPs que han accedit a la web i consten en llistes d'infraestructura maliciosa coneguda.

IPs malicioses han accedit a la web

3 IP que consten en llistes de reputacio maliciosa (botnets, atacants, sortides Tor) han fet peticions a la web.

3	3
IPs malicioses que han accedit	amb reputació negativa

IP	PAÍS / ASN	CATEGORIA	FONT	PETICIONS
203.0.113.77		Atacant	blocklist_de	296
198.51.100.23		Atacant	abuseipdb	419
192.0.2.150		Sortida Tor	tor	122

S'han detectat 3 adreces IP amb una reputació maliciosa que han accedit al lloc web durant el període d'anàlisi. D'aquestes, dues són classificades com a atacants (una de la font *blocklist_de* i una altra de *abuseipdb*), i una és una sortida de la xarxa Tor. Aquestes adreces han fet un total de 837 peticions, la majoria d'elles repetides i amb risc alt. Aquest tipus d'activitat és comú en qualsevol web exposada a Internet i indica que el lloc és un objectiu per a atacants automàtics, però no necessàriament que estigui compromís. No s'han detectat connexions amb servidors de comandament i control (C2) de malware, però el nivell global de risc del lloc web és ALTO, per tant aquesta activitat hostil ha de ser tractada amb atenció.

NIVELL DE RISC

El tràfic hostil entrant, com el detectat amb aquestes adreces IP, és una realitat quotidiana per a qualsevol web connectat a Internet. No implica necessàriament que el lloc estigui compromís, però sí que és un senyal que està sent atacat. El risc més greu, que seria la comunicació amb C2 de malware, no s'ha detectat en aquest cas. No obstant això, el nivell global de risc del lloc web és ALTO, per tant aquesta activitat hostil ha de ser tractada com una part del risc general. Aquesta secció, aïlladament, és menys alarmant, però el nivell global del lloc web segueix sent ALTO.

COM MITIGAR-HO

Anàlisi de SWPANEL.COM generat per SWPanel

Trànsit i indicadors de xarxa maliciosos

1

Activa la CDN de Cloudflare

URGENT

La CDN de Cloudflare pot ajudar a filtrar tràfic maliciós, bots i adreces IP suspicaces abans que arribin al servidor. Aquesta funció es pot activar directament des del SWPanel, sense necessitat de comandes tècniques.

2

Configura Fail2Ban gestionat

El Fail2Ban gestionat ja està actiu i pot ajudar a bloquejar automàticament adreces IP que mostren comportaments d'atac, com ara intents de forçar contrasenyes.

3

Bloqueja manualment les adreces IP detectades

Les adreces IP amb risc alt han de ser bloquejades manualment al servidor per evitar que tornin a accedir.

```
iptables -A INPUT -s 192.0.2.150 -j DROP
```

4

Monitoritza el tràfic d'entrada

És important revisar regularment els logs d'accés per detectar patrons d'atac o adreces IP noves amb comportament sospitós.

5

Revisa les configuracions de seguretat del lloc

Assegura't que totes les vulnerabilitats conegudes estiguin corregides i que el lloc estigui actualitzat.

Anàlisi de SWPANEL.COM generat per SWPanel

16

Risc per pais de l'origen del trafic

D'on venen les peticions al teu lloc i quin risc te cada pais d'origen, segons el volum d'IPs malicioses allotjades alli.

Anàlisi de SWPANEL.COM generat per SWPanel

Risc per pais de l'origen del trafic

D'on venen les peticions al teu lloc i quin risc te cada pais d'origen, segons el volum d'IPs malicioses allotjades alli.

PAISOS AMB MES INFRAESTRUCTURA MALICIOSA (RANQUING GLOBAL)

CODI	PAIS	PUNTS	BANDA	CATEGORIA PRINCIPAL
US	United States of America	100	Critic	abuse
CN	China	95,51	Critic	abuse
BR	Brazil	87,7	Critic	attacker
IN	India	86,14	Critic	attacker
GB	United Kingdom of Great Britain an	84,29	Alt	attacker
DE	Germany	82,96	Alt	abuse
CA	Canada	81,46	Alt	attacker
RU	Russian Federation	80,93	Alt	attacker
UA	Ukraine	80,52	Alt	abuse
AR	Argentina	79,8	Alt	abuse

PAISOS AMB MES CONCENTRACIO D'IPS MALICIOSES (DENSITAT)

CODI	PAIS	PUNTS	BANDA	DENSITAT
UZ	Uzbekistan	100	Critic	5256,7
MM	Myanmar	83,75	Alt	1306,18
AL	Albania	79,28	Alt	890,16
BD	Bangladesh	78,56	Alt	836,68
BW	Botswana	78,56	Alt	836,64
UA	Ukraine	78,36	Alt	822,64
LA	Lao People's Democratic Republic	77,69	Alt	776,75
BJ	Benin	77,6	Alt	770,53
NP	Nepal	76,5	Alt	701,38
ET	Ethiopia	75,66	Alt	652,4

Anàlisi de SWPANEL.COM generat per SWPanel

Risc per pais de l'origen del trafic

El trànsit del seu lloc web no ha pogut ser analitzat perquè no s'han registrat cap petició durant el període d'estudi. Això fa que no hi hagi dades disponibles per a determinar d'on prové el trànsit. No obstant això, cal recordar que el nivell general de risc del lloc web és ALTO, segons l'anàlisi global de totes les evidències recopilades. Aquesta valoració implica que, si el lloc comença a rebre trànsit, caldrà estar atents a l'origen geogràfic d'aquest, especialment si prové de països amb una alta densitat o volum de infraestructura maliciosa.

NIVELL DE RISC

Tot i que no hi ha hagut cap accés durant l'estudi, és important tenir en compte que els països amb una alta densitat de IPs malicioses, com Uzbekistan, Myanmar o Albania, podrien representar un risc elevat si el seu lloc comença a rebre trànsit d'aquests llocs. A més, països com els EUA, Xina o Brasil, tot i tenir menys densitat per milió d'IPs, tenen un volum global elevat d'infraestructura maliciosa, cosa que fa que qualsevol trànsit d'aquests llocs hagi de ser revisat amb atenció. Aquesta situació reforça el nivell general de risc ALTO del lloc web.

COM MITIGAR-HO

1

Activació de la CDN de Cloudflare

URGENT

La CDN de Cloudflare ha de ser activada des del SWPanel per afegir una capa de protecció entre Internet i el seu lloc web. Aquesta tecnologia filtra automàticament IPs malicioses, bots i atacants, i pot ajudar a reduir el trànsit hostil.

```
# Cap a SWPanel > Proteccions > CDN i activar Cloudflare
```

2

Configuració de regles de bloqueig manual

Si el trànsit comença a arribar i es detecten IPs o països amb risc elevat, es poden afegir regles de bloqueig manual mitjançant iptables.

```
# Exemple de comanda per bloquejar un IP:
iptables -A INPUT -s una IP no verificada -j DROP
```

3

Verificació del funcionament de Fail2Ban

Assegurar-se que el Fail2Ban gestionat està actiu i ben configurat per bloquejar automàticament atacants repetits.

Anàlisi de SWPANEL.COM generat per SWPanel

17

Matriu d’Impacte al Negoci

Traduïm cada incidència tècnica detectada a la seva conseqüència real per al teu negoci.

Anàlisi de SWPANEL.COM generat per SWPanel

Matriu d'Impacte al Negoci

Traduïm cada incidència tècnica detectada a la seva conseqüència real per al teu negoci.

INCIDÈNCIA	IMPACTE TÈCNIC	IMPACTE EN EL NEGOCI
Bucle d'errors PHP Detectat en aquest lloc	Escriptura massiva al registre d'errors i consum continu de processos PHP de la teva subscripció.	**Pèrdua de clients:** el web respon lent o mostra pantalles en blanc intermitents.
Injecció de codi o programari maliciós Detectat en aquest lloc	Funcions no autoritzades executant ordres i fils en segon pla.	**Dany de reputació:** Google pot penalitzar o desindexar el web, o els antivirus bloquejar l'accés a les teves visites.
Consultes SQL fallides Detectat en aquest lloc	Incapacitat de llegir o escriure registres al motor de base de dades.	**Pèrdua de vendes:** formularis que no s'envien i cistelles que fallen en el pagament.

Anàlisi de SWPANEL.COM generat per SWPanel

18

Conclusions

Què significa tot això per a tu, explicat de manera senzilla.

Anàlisi de SWPANEL.COM generat per SWPanel

Conclusions

Què significa tot això per a tu, explicat de manera senzilla.

El teu lloc web, **swpanel.com**, està en un estat de risc **ALTO**, i cal actuar aviat per protegir-lo. Aquest risc no és només tècnic, sinó que afecta la seguretat dels teus usuaris, la integritat dels teus dades i la confiança dels visitants. El que hem trobat és com si tinguessis una casa amb portes entreobertes, finestres sense clau i un sistema d'alarma que no funciona del tot. Això no vol dir que el lloc estigui totalment compromís, però sí que hi ha riscos reals que cal atendre immediatament.

El problema principal és que el lloc està rebent atacs reals: hi ha intents de forçar contrasenyes, provar injeccions SQL, i buscar fitxers sensibles com si fossin rastres de robatori. A més, el codi del lloc té errors que poden fer-lo més vulnerable, i alguns plugins estan desactualitzats, cosa que afeblit la seguretat. Els atacants estan intentant entrar, i si no els aturam ara, poden fer malbé el lloc o fins i tot robar dades.

Tot això passa perquè el lloc no té cap protecció avançada com una xarxa de distribució de contingut (CDN) o un sistema de detecció automàtica de riscos. A més, alguns fitxers clau tenen errors que poden fer que el lloc es torni més lliure d'atacs. No és un problema de sort, sinó de configuració i manteniment.

Tot i això, no cal alarmar-se. Els riscos són reals, però gestionables. El que cal és actuar amb prioritats clares: tancar les portes obertes, actualitzar allò que es pot i afegir capes de protecció addicionals. No és un problema de dies, però sí de setmanes si es fa bé. I si el lloc no es manté, aquestes situacions es tornen més greus amb el temps.

Ara mateix, tens el control per començar a resoldre-ho. El primer pas és actuar sobre allò que és més urgent, i després seguir amb allò que pot esperar. No estàs sol: amb aquest pla, pots tornar el lloc més segur i preparat per fer front a aquests riscos.

QUÈ HEM TROBAT · PER GRAVETAT

MITJÀ

5 errors de codi

Errors crítics en el codi que afeblis la seguretat

Hi ha 5 errors en 4 fitxers, com errors de tipus de dades, accés a propietats nul·les i esgotament de memòria. Aquests errors poden fer que el lloc es torni més vulnerable a atacs.

MITJÀ

Intent de forçar accés a dades sensibles

S'han detectat 23 intents d'injecció SQL i XSS, com provar d'obtenir contrasenyes o executar codi maliciós. Això vol dir que algú intenta accedir a informació privada.

Anàlisi de SWPANEL.COM generat per SWPanel

Conclusions

MITJÀ

1.312 peticions

Rastreig agressiu de fitxers sensibles

S'han detectat 1.312 intents de buscar fitxers com .env o wp-config.php.bak, que poden contenir dades clau com contrasenyes o claus d'API.

MITJÀ

Atacs de força bruta a l'administrador

S'han detectat 418 intents de forçar accés a wp-login.php i xmlrpc.php, que són portals clau per entrar al lloc.

MITJÀ

2 errors BD

Errors de base de dades que afecten la funcionalitat

Hi ha 2 errors de base de dades, com columnes inexistentes, que poden fer que certes funcions deixin de funcionar correctament.

ALT

2 per actualitzar

Plugins desactualitzats amb vulnerabilitats conegudes

2 plugins o temes estan desactualitzats, i un d'ells té una vulnerabilitat coneguda (CVE) amb puntuació 5.4, que pot ser explotada si no s'actualitza.

PLA D'ACCIÓ · PASSOS A SEGUIR

1

Revisar i corregir els errors crítics del codi

URGENT

Cal corregir els 5 errors de codi en 4 fitxers, especialment els que causen esgotament de memòria o accés a propietats nul·les. Això evitarà que el lloc es torni més vulnerable.

2

Actualitzar els plugins i temes desactualitzats

S'han detectat 2 plugins o temes desactualitzats, un dels quals té una vulnerabilitat coneguda. Cal actualitzar-los perquè no es pugui aprofitar aquesta brecha.

3

Activar la CDN de Cloudflare per protegir el lloc

La CDN de Cloudflare filtra bots, IP malicioses i atacs abans que arribin al servidor. És una capa de protecció essencial i fàcil d'activar des del SWPanel.

Anàlisi de SWPANEL.COM generat per SWPanel

Conclusions

4

Configurar regles de bloqueig manual d'IPs a iptables

Com que el servei no és un Cloud, cal configurar manualment regles de bloqueig d'IPs agressives. Per exemple, afegir aquestes IP a iptables per evitar que tornin a atacar.

```
iptables -A INPUT -s 203.0.113.45 -j DROP
iptables -A INPUT -s 198.51.100.23 -j DROP
iptables -A INPUT -s 203.0.113.77 -j DROP
iptables -A INPUT -s 192.0.2.150 -j DROP
```

5

Revisar i corregir els errors de base de dades

Els 2 errors de base de dades afecten la funcionalitat. Cal revisar la consulta SQL i assegurar-se que la columna 'plan_slug' existeix i està correctament referenciada.

6

Revisar els logs i configurar un sistema de bloqueig automàtic

Amb el Fail2Ban actiu, es poden configurar regles per bloquejar automàticament IP que facin molts intents de login o atacs. Això ajuda a reduir la càrrega del servidor i a protegir el lloc.

Entenc que aquesta situació pot semblar complexa, però no és impossible de resoldre. El que cal és actuar amb calma, prioritats clares i pas a pas. El primer pas és revisar els errors de codi i actualitzar allò que es pot. Després, afegir capes de protecció com la CDN i regles de bloqueig manual. Aquestes accions et permetran tornar el lloc més segur i preparat per fer front a aquests riscos.

Si tens dubtes o necessites ajuda per fer qualsevol dels passos, estic aquí per acompanyar-te. No cal fer-ho tot sol. Amb aquest pla, pots començar a actuar aviat i assegurar-te que el lloc torni a estar protegit. El primer pas és revisar els errors de codi i actualitzar els plugins. Si vols, podem començar-hi ara.

Anàlisi de SWPANEL.COM generat per SWPanel

Glossari de termes

Breu explicació dels termes tècnics utilitzats en aquesta anàlisi.

Backdoor (porta del darrere)
codi ocult que permet a un atacant accedir i controlar el lloc web de forma remota.

Cloaking
mostrar als cercadors un contingut diferent del que veuen els visitants; típic de l'spam SEO.

Codis d'estat HTTP (404, 5xx)
404 = pàgina no trobada; 5xx = error del servidor en processar la petició.

Força bruta
intents massius d'endevinar una contrasenya provant moltes combinacions.

Injecció (SQL / URL)
introduir codi o ordres a través d'un camp o una URL per executar accions no previstes.

Ofuscació
tècnica per amagar què fa realment el codi (per exemple amb base64_decode) i evitar-ne la detecció.

Permisos de BD (GRANT)
privilegis que determinen què pot fer un usuari a la base de dades (INSERT, UPDATE...).

Quantització
compressió del model del Motor IA de SWPanel perquè ocupi menys memòria mantenint gairebé la mateixa precisió.

Spam SEO
pàgines o enllaços injectats (apostes, farmàcia...) per posicionar contingut fraudulent al teu domini.

Timeout
la petició triga massa i s'interromp abans de completar-se.

Token
unitat mínima de text (paraula o fragment) que processa el Motor IA de SWPanel; mesura el volum de càlcul.

Transient (WordPress)
dada temporal que WordPress desa en memòria cau a la base de dades.

Veredicte (Net / Sospitós / Compromès)
classificació de seguretat que l'anàlisi assigna a cada fitxer.

Anàlisi de SWPANEL.COM generat per SWPanel

Glossari de termes

Webshell
script maliciós que dóna a l'atacant una consola per executar ordres al servidor.

Anàlisi de SWPANEL.COM generat per SWPanel

Estadístiques tècniques

Recursos i còmput invertits per generar aquesta anàlisi: descàrrega i anàlisi de logs i inferència del Motor IA de SWPanel.

Temps d'execució

9m 52s	6m 28s	3m 24s
TEMPS TOTAL	TEMPS D'ANÀLISI	CONFECCIÓ DEL PDF

Logs analitzats

14	186.420	39,93 MB
LOGS DESCARREGATS	LÍNIES ANALITZADES	DADES PROCESSADES

els logs proporcionats
CAPES REVISADES

Errors i correccions

5	4	4
ERRORS ÚNICS	FITXERS AFECTATS	CORRECCIONS

2
ERRORS CRÍTICS

Còmput del Motor IA de SWPanel

8	13.715	7.382
CRIDES AL MODEL	TOKENS D'ENTRADA	TOKENS GENERATS

21.097	~54 tok/s
TOKENS PROCESSATS	VELOCITAT DE GENERACIÓ

Anàlisi de SWPANEL.COM generat per SWPanel

Estadístiques tècniques

Motor IA de SWPanel (anàlisi i redacció)

qwen3-coder MOTOR IA DE SWPANEL	**qwen3moe** FAMÍLIA	**30.5B** PARÀMETRES
Q8_0 QUANTITZACIÓ		

Infraestructura de còmput

NVIDIA A100 GPU	**6.912** NUCLIS GPU (CUDA)	**432** TENSOR CORES
80 GB HBM2e VRAM	**2 TB/s** AMPLE DE BANDA	**19,5 TFLOPS** FP32
312 TFLOPS FP16/BF16	**221.184** FILS CUDA	**80** FILS DE CPU

Energia consumida i el seu cost

0,062 kWh CONSUM IT (SERVIDOR + GPU)	**0,093 kWh** REFRIGERACIÓ (X1,5)	**0,155 kWh** ENERGIA TOTAL
0,19 € COST DE CÒMPUT		

Cost d'infraestructura (amortització)

0,61 € AMORTITZACIÓ HW I XARXA	**0,155 kWh** ENERGIA D'INFRAESTRUCTURA	**38 g** CO2 D'INFRAESTRUCTURA

Anàlisi de SWPANEL.COM generat per SWPanel

Estadístiques tècniques

0,83 €
COST TOTAL ESTIMAT

77 g
CO2 ESTIMAT

COM S'HAN CALCULAT AQUESTES XIFRES

Mètriques estimades sobre infraestructura NVIDIA NVIDIA A100 amb el model qwen3-coder:30b-a3b-q8_0. El consum mitjà del servidor amb la GPU és d'uns 575 W. La refrigeració afegeix 1,5 kW per cada kW de còmput, de manera que el consum total és ~1,5 vegades el de còmput (PUE 1,5). L'energia es calcula sobre el temps real d'anàlisi a 0,185 EUR/kWh, el cost de còmput a tarifa cloud de referència (~1,8 EUR/h) i el CO2 a 250 g/kWh. Valors aproximats per dimensionar l'esforç d'aquesta anàlisi.

TECNOLOGIA EFICIENT

Aquesta anàlisi s'executa en infraestructura pròpia amb el Motor IA de SWPanel (models locals), sense enviar el teu codi a tercers. Detectar i corregir els errors aviat evita reprocessos, pàgines caigudes i consum innecessari de recursos del servidor.

UN GEST D'AMOR PEL PLANETA

Crear aquest informe ha deixat una petjada d'uns 77 g de CO2. Darrere de cada anàlisi hi ha energia, aigua i recursos de l'única casa que tots compartim. Et demanem un petit acte d'amor: demana només els informes que realment necessitis i evita imprimir-los, per tenir cura dels boscos, l'aire i la vida dels qui vindran després. Tenir cura de la Terra és tenir cura els uns dels altres. Gràcies, de cor, per deixar una petjada més lleugera i un demà més verd.

Anàlisi de SWPANEL.COM generat per SWPanel

swpanel

https://www.swpanel.com

Document: SW-COD-EJEMPLO-2026

Data: 16/10/2026