mySites.guru

# Smart Slider 3 Hack Allows Any File to Be Downloaded

CVE-2026-3098 lets any subscriber download wp-config.php from 800,000 WordPress sites running Smart Slider 3. How to check and fix it.

Phil E. Taylor | 16 April 2026

Critical update — April 8, 2026

### Smart Slider 3 Pro ~~3.5.1.35~~ was a supply-chain attack

Since this post was published, a security breach affected the update infrastructure responsible for distributing Smart Slider 3 updates. Unauthorized parties published a malicious version **3.5.1.35**, which may have been installed on some websites before the issue was detected. The compromised release contains a remote code execution backdoor that runs shell commands or arbitrary PHP via a single query parameter, and it affects **both the WordPress and Joomla editions** of Smart Slider 3 Pro.

If your site is currently on 3.5.1.34 (the version this post recommended last week), you are still safe, but you must **skip 3.5.1.35 entirely and update directly to 3.5.1.36 or later**. If your site ran 3.5.1.35 at any point, treat it as compromised: run the indicator-of-compromise checks and use Nextend's official cleanup script.

| LAST SAFE | COMPROMISED | UPDATE TO |
|---|---|---|
| 3.5.1.34 | ~~3.5.1.35~~ | 3.5.1.36+ |

Read the full supply-chain compromise post →

Smart Slider 3, one of the most popular slider plugins for WordPress with over 800,000 active installations, has a vulnerability that lets any registered user download **any file from your server**. Not just images or slider assets. Any file the web server process can read.

`wp-config.php` with your database credentials. `/etc/passwd`. Your `.env` file. Private SSL keys. Database backup files sitting in a directory someone forgot to protect. Payment gateway configs. SMTP credentials. If it's on the filesystem and readable by the web server, an attacker with nothing more than a free subscriber account can download it.

The vulnerability (CVE-2026-3098, CVSS 6.5 Medium) affects all versions up to and including 3.5.1.33. If you run Smart Slider 3, update to ~~version 3.5.1.34~~ `3.5.1.36+` now.

This was first reported by Wordfence, but their disclosure doesn't mention Joomla once. Smart Slider 3 also ships as a Joomla extension, and we've confirmed it shares the same vulnerable codebase - identical files, identical hashes. If you manage Joomla sites, read the Joomla section below.

## TL;DR

- **CVE-2026-3098** - CVSS 6.5 arbitrary file read in Smart Slider 3 versions up to 3.5.1.33
- Any subscriber-level user can download any file the web server can read: `wp-config.php`, `.env`, `/etc/passwd`, private keys, database backups, payment configs
- Update to ~~Smart Slider 3.5.1.34~~ — now use `3.5.1.36+`
- After updating, regenerate your authentication keys/salts and change your database password
- Sites with open user registration are at highest risk

> **Update now. Don't wait.**
>
> This vulnerability is public knowledge. The exploit requires only a free subscriber account. If your site allows any form of user registration, every minute you wait is a minute an attacker could be downloading your database credentials, private keys, and every other sensitive file on your server.

## How Many mySites.guru Users Are Affected by Smart Slider 3?

We checked our database this morning. Across the thousands of agencies using mySites.guru:

| 724 | 7,869 |
| --- | --- |
| Agencies affected | Sites running vulnerable versions |

Every one of those agencies already has a warning in their mySites.guru dashboard, because the Wordfence Vulnerability API is built into the platform and flagged it automatically. All 724 are being emailed today.

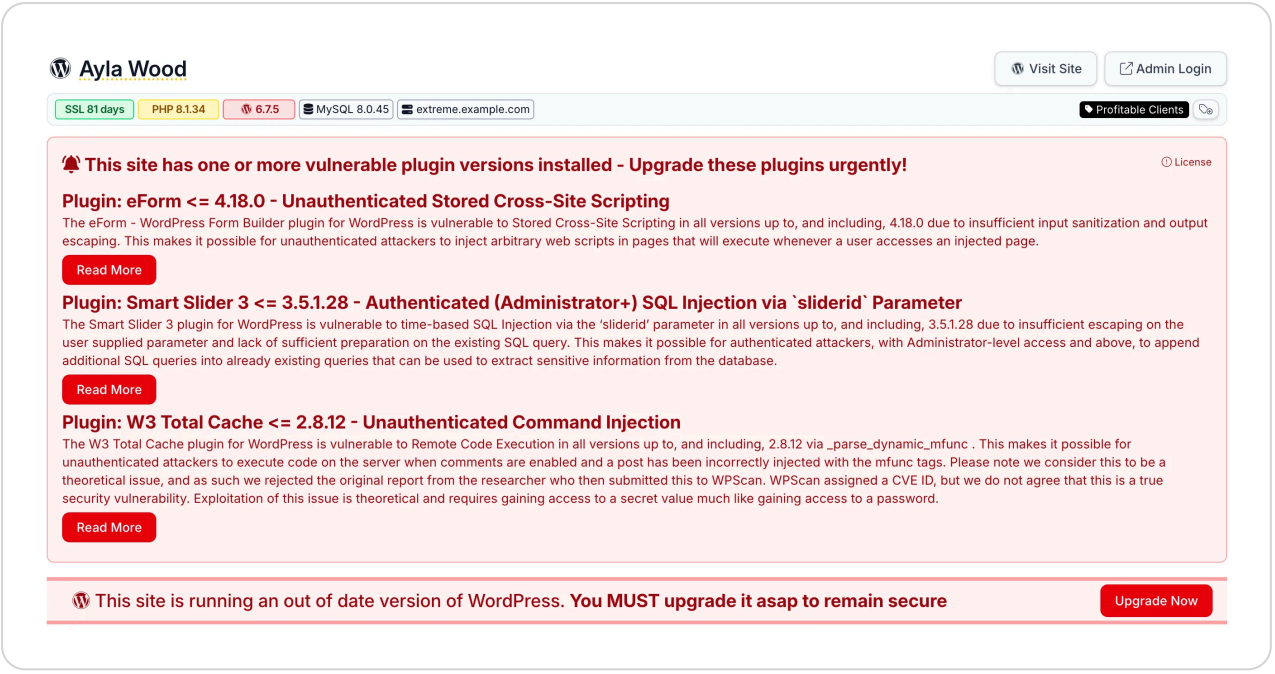
Those 724 agencies didn't need to read this post to know they had a problem. They already knew.

## How Does the mySites.guru Detection of Smart Slider 3 Work?

Twice a day, a snapshot runs on each connected WordPress site, collecting every installed plugin and its version number. That list gets cross-referenced against Wordfence, CVE/Mitre, and custom threat intelligence databases.

If your site runs Smart Slider 3 version 3.5.1.33 or earlier, it gets flagged with the specific CVE, severity rating, and a direct link to the advisory. No manual checking required.

This isn't the first time mySites.guru has flagged Smart Slider 3 either. The plugin had a previous SQL Injection vulnerability (CVE-2025-6348) in versions up to 3.5.1.28 that was also caught automatically. Here's what the vulnerability warning looks like in the mySites.guru dashboard:

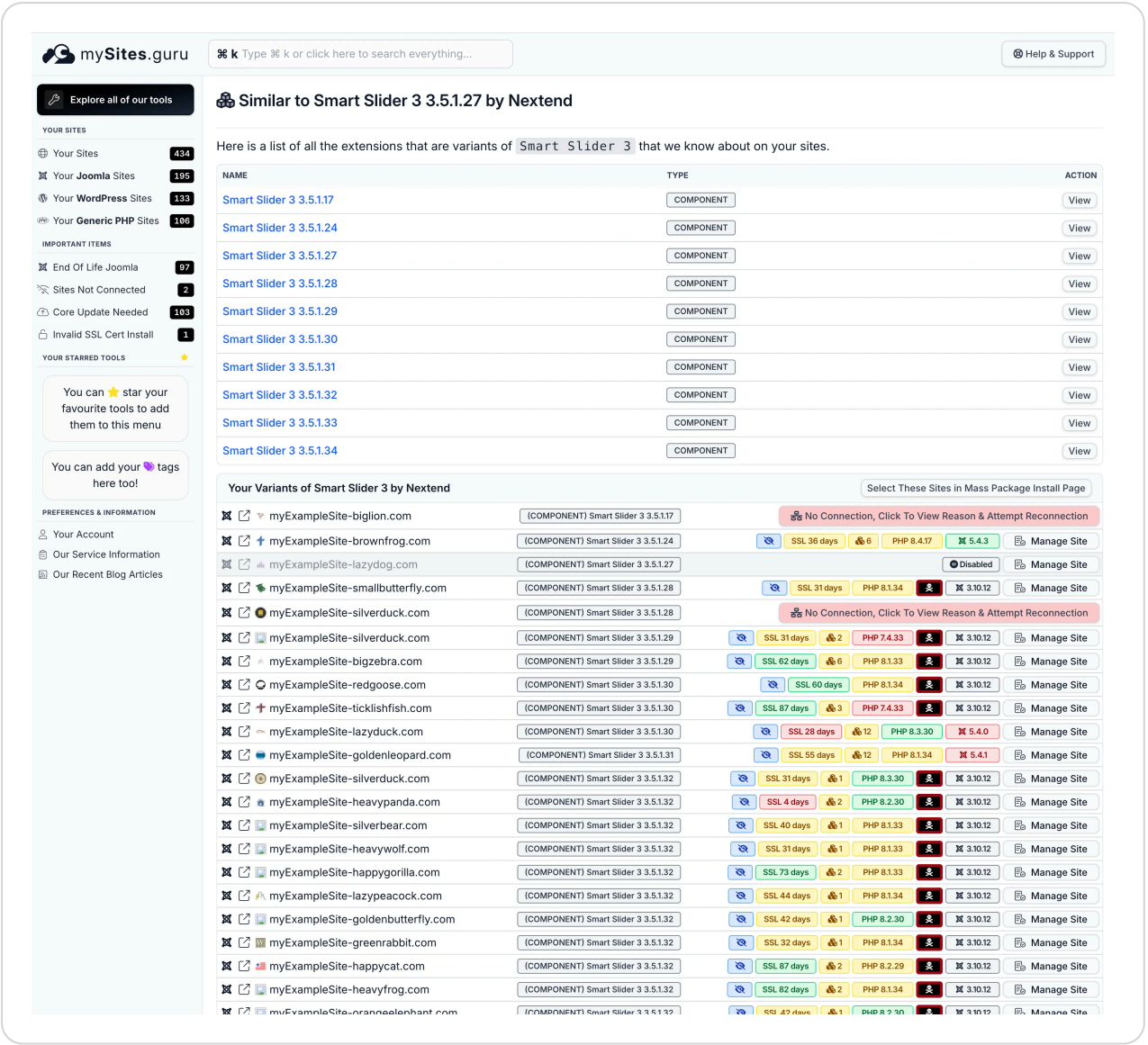



Every vulnerable plugin version gets its own entry with the full advisory text, so you know exactly what the risk is before deciding how urgently to patch.

## How to Quickly Find Which Sites Have Smart Slider 3 Installed with mySites.guru

When a vulnerability like this drops, the first question is: “Which of my sites have this installed?” If you manage 50 or 200 client sites, you don’t have time to log into each one and check the plugins page.

mySites.guru indexes every plugin on every connected site. One URL gives you the complete list of every site running Smart Slider 3, broken down by version number, with the site’s PHP version, WordPress version, and SSL status alongside it:




If you're already a mySites.guru subscriber, you can open this page right now:

### View all your Smart Slider 3 installations

**Open Smart Slider 3 Extension Search**

Lists every version installed across all your connected sites, grouped by version number. You'll see which sites are still on vulnerable versions at a glance.

Every version of Smart Slider 3 installed across your sites is listed at the top. Below that, every individual site running the plugin, with its exact version. You can see which sites are still on vulnerable versions and which have already been updated to 3.5.1.34.

That turns a vulnerability announcement from a stressful afternoon of logging into admin panels into a five-minute triage. One page, you know exactly which clients are exposed, and you start patching.

### How to Push the Smart Slider 3 Update Across All Your Sites

Once you know which sites are affected, the mass plugin updater lets you select every site running the vulnerable version and push the update in one batch. When a vulnerability drops affecting 800,000 sites, the agencies that patch in hours rather than weeks are the ones that don't end up in incident response.

If you don't have a mySites.guru account yet, sign up for a free trial and connect your sites. The plugin index builds automatically on the first snapshot.

## What Happened with Smart Slider 3 CVE-2026-3098?

The vulnerability was discovered by Dmitrii Ignatyev on February 23, 2026, and reported through the Wordfence Bug Bounty Program (earning a $2,208 bounty). Wordfence validated the proof-of-concept the next day and notified the developer, Nextend.

The problem is a missing capability check in Smart Slider 3's export functionality. The plugin's AJAX actions that handle slider exports are protected by a nonce (a one-time token that proves the request came from a logged-in session), but there's no check on whether the user actually has permission to use that feature.

A nonce proves you're logged in. It doesn't prove you're an admin.

In the vulnerable version, any authenticated user, including someone with just a subscriber account, could:

1. Obtain the required nonce (it's available to any authenticated user)
2. Call the `actionExportAll` function via AJAX
3. Receive a ZIP file containing exported slider data, including any referenced files

The `ExportSlider` class's `create()` method adds files to the export ZIP using `file_get_contents()` without validating file types or restricting which directories can be accessed. Image files, video files, PHP files, config files, private keys - everything is treated the same way. There is no allowlist, no path restriction, and no file extension check. An attacker can manipulate the export to include any file the web server process can read.

> **Important: this is not limited to wp-config.php**
>
> Any file readable by the web server is exposed. That includes `.env` files, `/etc/passwd`, database backups, SSL private keys, payment gateway configs, SMTP credentials, and any other sensitive file on the server. If you run Smart Slider 3 on a shared hosting account, other sites on the same server may also be at risk depending on your host's isolation setup.

## Why Is the Smart Slider 3 File Read So Dangerous?

`wp-config.php` gets the most attention because it contains everything an attacker needs to own your site, but most servers have sensitive files well beyond WordPress configs.

A single read of `wp-config.php` gives an attacker:

- Database username, password, host, and database name. If the database port is accessible from outside the server (more common than you'd think on budget hosting), they can connect directly and pull user password hashes, customer data, WooCommerce orders, and private content.
- Authentication keys and salts - the eight constants (`AUTH_KEY`, `SECURE_AUTH_KEY`, `LOGGED_IN_KEY`, `NONCE_KEY`, and their corresponding salts) that WordPress uses to sign session cookies. With these values, an attacker can forge a valid admin session cookie without knowing the admin password.
- The table prefix, which makes SQL injection attacks against other vulnerabilities more precise.
- Any third-party secrets stored as constants: API keys, payment gateway credentials, SMTP passwords, cloud storage keys. Many plugins put these in `wp-`

`config.php`.

The practical attack chain: forge an admin cookie using the stolen keys, log into wp-admin, install a backdoor plugin, and maintain persistent access even after the original vulnerability is patched.

## Who Is at Risk from the Smart Slider 3 Vulnerability?

The vulnerability requires subscriber-level authentication, the lowest role in WordPress. This means:

- WooCommerce stores, where customers create accounts to place orders (subscriber access)
- Membership sites and anything using a registration plugin
- Any site with "Anyone can register" enabled in Settings > General
- Multisite networks, where user registration on any site in the network provides the access level needed
- Sites with compromised low-privilege accounts from a previous breach or credential stuffing attack

If your site doesn't allow any form of user registration and has no subscriber accounts, the risk is significantly lower (but not zero, since an attacker could exploit a separate vulnerability to create an account first).

## What Should You Do About Smart Slider 3 Right Now?

### 1. Update Smart Slider 3 to ~~3.5.1.34~~ 3.5.1.36 or Later

The 3.5.1.34 patch adds capability checks to the export AJAX actions and originally fixed CVE-2026-3098. However, **version 3.5.1.35 was a malicious supply-chain release** containing a remote code execution backdoor. Always install **3.5.1.36 or newer** to get both the CVE fix and a clean codebase. Update through the WordPress plugin

updater or download from wordpress.org. See the supply-chain compromise post for the full background.

If you manage multiple sites, use the mySites.guru mass updater to push the update everywhere at once.

## 2. Regenerate Your Authentication Keys and Salts

If there's any chance the vulnerability was exploited before you patched, your keys and salts should be considered compromised. Generate new ones at api.wordpress.org/secret-key/1.1/salt/ and replace the existing values in `wp-config.php`. This immediately invalidates all active sessions, forcing every user (including any attacker with a forged cookie) to log in again.

## 3. Change Your Database Password

Update the password in your hosting control panel or database server, then update `DB_PASSWORD` in `wp-config.php` to match. If the attacker read your credentials, this cuts off direct database access.

## 4. Audit Your User Accounts

Check your WordPress user list for accounts you don't recognize, especially subscribers. Delete any unauthorized accounts. If you manage multiple sites, mySites.guru's user management lets you review accounts across all your sites from one place.

## 5. Run a Security Audit

Use the mySites.guru suspect content scanner to check for backdoors or modified files. If an attacker escalated from file read to admin access using forged cookies, they may have left persistent backdoors that survive the plugin update.

Set up real-time file change monitoring so you'll be alerted immediately if any watched files are modified after cleanup.

### 6. Review Server Access Logs

Check your access logs for unusual requests to Smart Slider 3's AJAX endpoints. Look for POST requests to `admin-ajax.php` with actions related to slider export from IP addresses you don't recognize. This can help determine whether the vulnerability was exploited before the patch.

## Smart Slider 3 Has a History of Vulnerabilities

This isn't a one-off. Smart Slider 3 has had eight documented vulnerabilities since 2021, including two High-severity issues in 2022. If you're running this plugin, you need to stay on top of updates.

| Year | CVE | Type | CVSS | Min. Role | Fixed In |
|---|---|---|---|---|---|
| 2021 | CVE-2021-24382 | Stored XSS | 4.8 | Author | 3.5.0.9 |
| 2022 | CVE-2022-3357 | PHP Object Injection | 8.1 | Subscriber | 3.5.1.11 |
| 2022 | CVE-2022-45843 | Stored XSS | 5.4 | Contributor | 3.5.1.11 |
| 2022 | CVE-2022-45845 | Deserialization of Untrusted Data | 8.8 | Subscriber | 3.5.1.11 |
| 2023 | CVE-2023-0660 | Stored XSS | 6.8 | Contributor | 3.5.1.14 |
| 2024 | CVE-2024-3027 | Missing Auth / File Upload | 6.4 | Subscriber | 3.5.1.23 |
| 2025 | CVE-2025-6348 | SQL Injection via `sliderid` | 7.6 | Admin | 3.5.1.29 |
| 2026 | CVE-2026-3098 | **Arbitrary File Read** | **6.5** | **Subscriber** | **3.5.1.34** |

Notice the pattern: three of these eight vulnerabilities (including the current one) require only **subscriber-level access**. That's the lowest authenticated role in WordPress. The 2022 PHP Object Injection (CVSS 8.1) and Deserialization (CVSS 8.8) issues were both subscriber-exploitable too.

The vendor has patched every disclosed vulnerability, and the response time on CVE-2026-3098 (acknowledged March 2, patched March 24) was reasonable. But the

recurring pattern, especially around subscriber-level exploits, is something to factor into your risk assessment if you're deciding whether to keep using this plugin.

## Is the Joomla Version of Smart Slider 3 Also Vulnerable?

Yes. Smart Slider 3 is available for both WordPress and Joomla, and they share the same Nextend framework codebase. We compared the patched Joomla release (3.5.1.34) against the patched WordPress release and found **identical files** - the md5 hashes of both `ExportSlider.php` and `ControllerSliders.php` match exactly between platforms.

The vulnerable code path is the same on both platforms: the `actionExportAll()` method lacked a permission check, and `ExportSlider::create()` had no file extension whitelist. The 3.5.1.34 patch adds `validatePermission('smartslider_edit')` and restricts exported files to image and media extensions (jpg, png, gif, mp4, mp3, svg, webp, avif).

The Smart Slider 3 changelog is unified across both platforms, and the 3.5.1.34 entry ("Fix: Vulnerability improvements") applies to WordPress and Joomla equally. Earlier entries in the same changelog reference Joomla-specific features like Joomla 6 compatibility, VirtueMart generators, and Joomla article generators, confirming this is a single shared codebase.

If you run Smart Slider 3 on Joomla sites, update to ~~3.5.1.34~~ ❗ `3.5.1.36+` with the same urgency. The Wordfence disclosure focuses on WordPress, but the Joomla version carries identical risk.

This is a recurring pattern for cross-platform plugins. The same thing happened with AcyMailing CVE-2026-3614 in April 2026: a WordPress-only CVE, a vendor patch that covers both CMS platforms, and no advisory reaching the Joomla half of the affected installations. If you run Joomla sites with plugins that also ship a WordPress build, watch the WordPress CVE feeds too.

## Other WordPress Slider Plugins Have the Same Problem

Smart Slider 3 isn't alone. In October 2025, Wordfence disclosed a similar arbitrary file read in Slider Revolution affecting 4 million sites. That vulnerability also allowed authenticated users to read arbitrary server files through the export functionality.

Slider plugins need file system access for exporting and importing configurations. That access, paired with missing authorization checks on export functions, is a recurring vulnerability pattern. The root cause in both cases: nonce validation without capability checks.

The same pattern appears on the Joomla side too. The Novarain/Tassos Framework vulnerability (CVE-2026-21627) disclosed in February 2026 is another AJAX endpoint with missing authorization, this time fully unauthenticated. Joomla's `com_ajax` routes requests to the nrframework plugin, which whitelists file inclusion as a non-admin task. No nonce, no login, no capability check at all. The root cause across all four vulnerabilities (Smart Slider 3, Slider Revolution, Novarain Framework, and now Joomla core itself) is the same: the AJAX handler authenticates the request but never authorises the action.

**Update (March 31, 2026):** Joomla 5.4.4 and 6.0.4 shipped with ACL hardening for `com_ajax` in Joomla core. The framework that routes AJAX requests for every Joomla plugin had the same authorization gap as the plugins built on top of it. This isn't a handful of careless developers - the pattern runs all the way down to the CMS itself. Extension developers who rely on `com_ajax` should audit their own authorization checks now.

## Smart Slider 3 CVE-2026-3098 Disclosure Timeline

| Date | Event |
|---|---|
| February 23, 2026 | Vulnerability submitted to Wordfence Bug Bounty by Dmitrii Ignatyev |
| February 24, 2026 | Wordfence validated the proof-of-concept |
| February 24, 2026 | Full details sent to Nextend (Smart Slider developer) |
| February 24, 2026 | Wordfence Premium/Care/Response users received a firewall rule |

| Date | Event |
| --- | --- |
| March 2, 2026 | Nextend acknowledged the report and began working on a fix |
| March 24, 2026 | Patched version 3.5.1.34 released |
| March 26, 2026 | Wordfence Free users received the firewall rule |

## Want Someone to Handle the Smart Slider 3 Fix for You?

If you'd rather hand this off, visit fix.mysites.guru and submit a request. For a one-time set fee, the site gets patched, audited, locked down, and handed back secure. Non-subscribers get a free month of mySites.guru included.

## Further Reading

- Wordfence advisory for CVE-2026-3098 - the original disclosure with full technical analysis
- Smart Slider 3 on WordPress.org - download the latest patched version
- WordPress Hardening Handbook - official security best practices
- Patchstack Smart Slider 3 vulnerability history - all eight documented CVEs
- WordPress secret key generator - regenerate your authentication keys and salts
- AJAX Endpoints: The Biggest CMS Security Blind Spot - the same nonce-without-capability pattern across Joomla's com_ajax and WordPress admin-ajax.php
- Four WordPress Plugins That Shipped Security Patches in March 2026 - Elementor, Yoast SEO, WPForms, and Really Simple Security all patched critical issues in the same disclosure window as CVE-2026-3098
- Ninja Forms File Uploads CVE-2026-0740 - another WordPress plugin admin-ajax.php handler that made it one step further, landing an unauthenticated arbitrary file upload (CVSS 9.8) affecting around 50,000 sites

For a broader look at CMS security, see our agency security guide.

# Frequently Asked Questions

### What is the Smart Slider 3 vulnerability CVE-2026-3098?

CVE-2026-3098 is a CVSS 6.5 Medium severity arbitrary file read vulnerability in Smart Slider 3 versions 3.5.1.33 and earlier. An attacker with a basic subscriber account can exploit the slider export function to download any file from the server, including wp-config.php which contains database credentials and authentication keys.

### How do I know if my site is affected by the Smart Slider 3 vulnerability?

If your site runs Smart Slider 3 version 3.5.1.33 or earlier, it is vulnerable to CVE-2026-3098. Check your plugin version in Plugins > Installed Plugins in wp-admin. Update directly to version 3.5.1.36 or later (skip 3.5.1.35, which was a malicious supply-chain release). mySites.guru's vulnerability alerting will flag this automatically on connected sites.

### Does the Smart Slider 3 vulnerability require admin access to exploit?

No. The vulnerability only requires subscriber-level access, the lowest authenticated role in WordPress. Any registered user on your site can exploit it. Sites with open registration, WooCommerce stores, or membership plugins are especially at risk.

### What can an attacker do with my wp-config.php file?

wp-config.php contains your database username and password, authentication keys and salts (used to sign session cookies), your table prefix, and often third-party API keys. An attacker can use these to connect to your database directly, forge admin session cookies, or escalate to full site takeover.

### Does mySites.guru detect the Smart Slider 3 vulnerability automatically?

Yes. mySites.guru has the Wordfence Vulnerability API built in and cross-references every installed plugin version twice daily. On the day of disclosure, 724 agencies managing 7,869 sites were automatically notified that their sites were running a vulnerable version of Smart Slider 3.

### What should I do after updating Smart Slider 3?

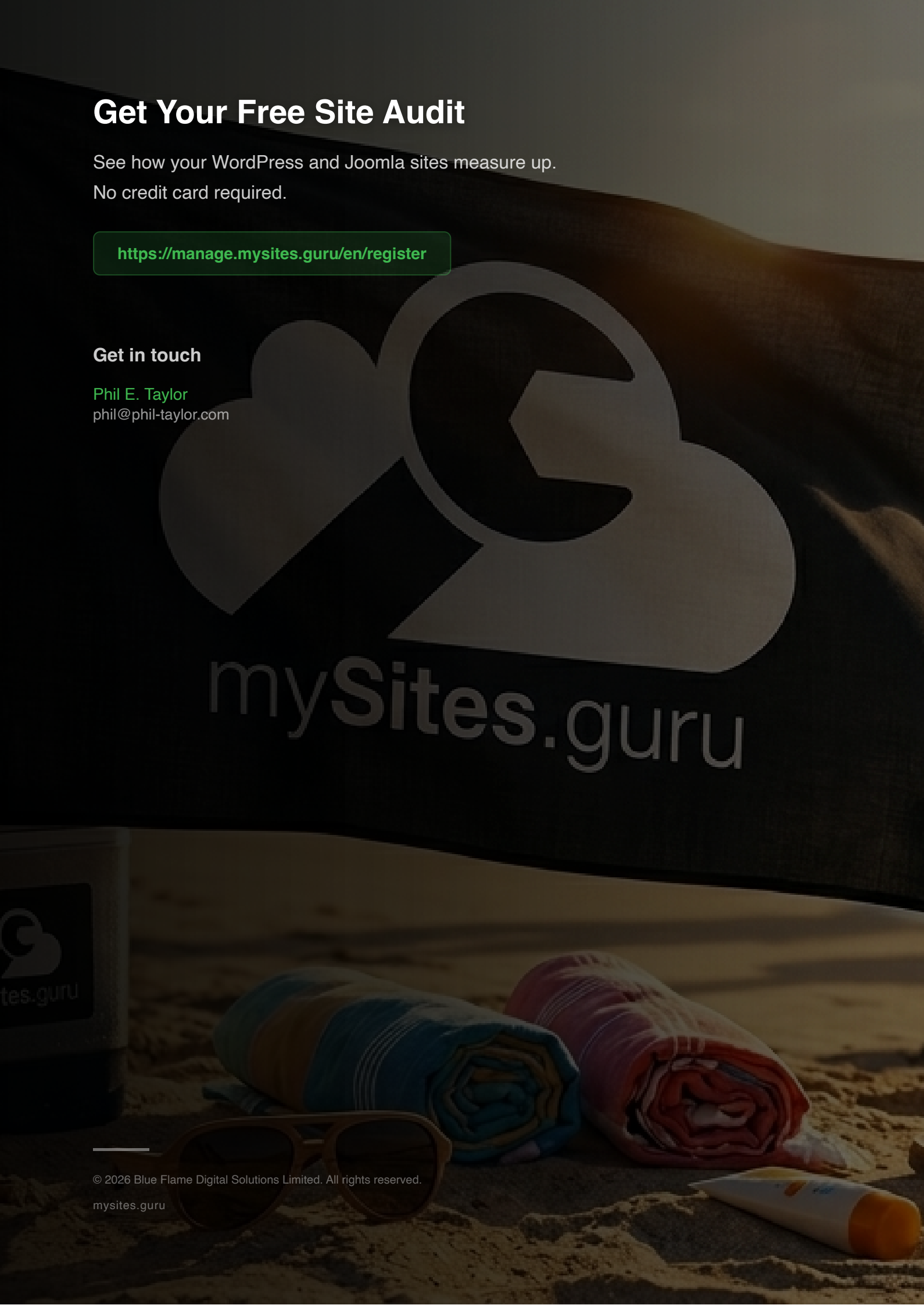
After updating to 3.5.1.36 or later (skip the malicious 3.5.1.35), regenerate your WordPress authentication keys and salts in wp-config.php. Change your database password. Review your user list for unauthorized subscriber accounts. Run a security audit to check for signs of prior exploitation.

# Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

**https://manage.mysites.guru/en/register**




### Get in touch

Phil E. Taylor
phil@phil-taylor.com