WordPress security advisory: Smart Slider 3 Pro 3.5.1.35 compromise

Description

A security breach affected the update system responsible for distributing **Smart Slider 3 Pro for WordPress**. Unauthorized parties released a malicious version **3.5.1.35**, which may have been installed on some websites.

Once detected, the update infrastructure was shut down and a full security audit was performed. A fixed and secure version **3.5.1.36** has been released.

⚠️ **Important: Only the Pro version is affected.**

The malware in the WordPress version differs from Joomla and includes deeper persistence mechanisms.

Affected Versions

Version	Status	Action Required
3.5.1.35	❌ Compromised	Immediate action required
3.5.1.36	✅ Safe	No action needed
≤ 3.5.1.34	✅ Safe	No action needed

🍪 We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextweb.com/privacy-policy/)

Great, I love cookies!

What the Malware Does (WordPress)

The malicious plugin version includes multiple backdoors and persistence layers.

It may:

- Execute system commands remotely via HTTP headers (`shell_exec`)
  Execute arbitrary PHP code via hidden request parameters
  Create a hidden administrator user:
  - username: `wpsvc_xxxx` , `wp_maint_xxxx`
  - email: `kiziltxt2@gmail.com`
    Hide this user from the admin interface
    Store credentials in WordPress options (`_wpc_uinfo`)
    Install persistent backdoors in multiple locations:
  - `wp-content/mu-plugins/object-cache-helper.php`
  - theme `functions.php`
  - `wp-includes/class-wp-locale-helper.php`
- Send site and credential data to an external server (`wpjs1.com`)

Because of this, affected sites should be considered **fully compromised**.

🔄 Server Rollback

If you have an available backup point, we strongly recommend rolling back your server to a backup created **before version 3.5.1.35**.

The compromised update was released by the attacker on **April 7, 2026**. Due to time zone differences, it is safest to restore from a backup dated **April 5, 2026 or earlier**.

This ensures that any potentially malicious files are completely removed, as they were never present in the restored backup.

How to Roll Back

1. Log in to your server hosting provider's dashboard
2. Look for a section related to **backups, snapshots, or restore points**
3. Find a backup created **before version 3.5.1.35 (April 5. or before that)**
4. Use the available **restore/rollback option** to restore that backup

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)
Great, I love cookies!

> ⚠️ *Backup and restore options vary between providers.*
>
> *If you're unsure how to proceed, please contact your hosting provider's support for assistance.*

Reset Your Credentials

After restoring your server, it is still recommended to regenerate:

- your security keys (#9-Clean-wp-configphp-and-htaccess-G-ur3) (salts) in the wp-config.php
- your credentials (#11-Change-All-Passwords-40pJr) as the attacker might have accessed them.

If you don't have a backup, then proceed with the manual cleanup methods described below.

🛠 Manual Cleanup Guide

Follow these steps carefully.

---

1. Update Immediately

- Reinstall Smart Slider, as you see here (//smartslider.helpscoutdocs.com/article/1752-update#Reinstall-Mfqno). So you should delete 3.5.1.35 and install 3.5.1.36. (Your sliders will stay!)

---

2. Put Site in Maintenance Mode

Temporarily restrict access to prevent further exploitation.

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

3. Backup the Site

Create a full backup of:

- Files
- Database

Label it as **infected backup**.

---

4. Remove Malicious Plugin

Delete the entire plugin directory:

```
wp-content/plugins/nextend-smart-slider3-pro/
```

⚠️ Do not leave any files behind.

---

5. Remove Hidden Admin User

Check all users in WordPress.

Look for:

- username starting with: `wpsvc_` or `wp_maint_`
- email: `kiziltxt2@gmail.com`

Delete these users immediately.

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy)

Great, I love cookies!

6. Remove Persistence Files

Delete these files if they exist:

```
wp-content/mu-plugins/object-cache-helper.php
wp-content/mu-plugins/wp-performance-toolkit.php

wp-includes/class-wp-locale-helper.php
wp-includes/class-wp-locale-textdomain.php

wp-includes/.cache_key
wp-includes/.lc_messages
```

These are hidden backdoors that allow re-entry.

---

7. Clean Theme `functions.php`

Check all active themes / child themes:

```
wp-content/themes/<your-theme>/functions.php
```

Remove any suspicious codes matching this malicious pattern, which enabled remote execution:

```
add_action('init',function(){ ... eval(...) ... shell_exec(...) ... });
```

Also look for:

- Code that recreates files inside `mu-plugins/`
- Any base64-encoded or obfuscated PHP code

⚠️ This is a critical step.

If this file is not cleaned, the malware can reinstall itself on every page load.

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

---

8. Remove Malicious WordPress Options

In database (`wp_options` table), delete:

- `_wpc_ak`
- `_wpc_uid`
- `_wpc_uinfo`
- `_perf_toolkit_source`
- `wp_page_for_privacy_policy_cache`

These may store attacker tokens, credentials, or hidden payloads.

---

9. Clean up the wp-config.php

Check your `wp-config.php` file.

Remove this constant if exists:

```
define('WP_CACHE_SALT', '<token>');
```

Change the WordPress Security Keys (Salts):

1. Generate new security keys here: https://api.wordpress.org/secret-key/1.1/salt/ (https://api.wordpress.org/secret-key/1.1/salt/)
2. Open your website's `wp-config.php` file
3. Replace the existing keys (AUTH_KEY, SECURE_AUTH_KEY, etc.) with the new ones (please make sure you won't add them twice, but you actually replace the existing salts with the new ones, as defining constants twice could causes errors)
4. Save the file

This will also log out all users and invalidate existing sessions.

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

10. Clean up the .htaccess

Check your `.htaccess` file in the WordPress root folder and remove the line if present:

```
# WPCacheSalt <token>
```

These may be used to store attacker tokens.

---

11. Reinstall WordPress Core

Replace all core files with a clean version:

- Download WordPress from official source
  Replace everything except:
  - `wp-config.php`
  - `wp-content/uploads/`

---

12. Reinstall Plugins and Themes

- Remove all plugins
- Reinstall only from trusted sources
- Remove unused or nulled plugins

---

13. Change All Passwords

Reset:

- WordPress admin passwords
- WordPress security keys (salts)
- Hosting account

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)
Great, I love cookies!

- FTP / SSH
- Database password
- Email accounts

How to reset the WordPress admin passwords:

1. Log in to your WordPress dashboard: `/wp-admin`
2. Go to **Users** → **All Users** (`/wp-admin/users.php`)
3. For each user with the **Administrator** role:
   a. Click **Edit**
   b. Scroll down to the **Account Management** section
   c. Click **Set New Password** (WordPress will generate a strong password automatically)
   d. Click **Update User** to save
4. Tip: You can also use the **“Send password reset”** option so each administrator can set their own password securely.

Changing the Database password:

Please contact your hosting provider for guidance on how to change your WordPress database user password.

After changing it:

1. Open `wp-config.php`
2. Update the value of this constant to the new password that you generated:

```
define( 'DB_PASSWORD', 'your-new-password');
```

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

Changing the FTP / SSH and Hosting account credentials:

Please contact your hosting provider for guidance on how to change these credentials.

14. Scan for Additional Malware

Search for:

- `eval(base64_decode`
- `shell_exec`
- `_wpc_`
- `wpjs1.com`

Check especially:

- `wp-content/`
- `uploads/`
- `cache/`
- `mu-plugins/`
- `themes/`

15. Review Logs

Check:

- access logs
- admin logins
- unusual POST requests

Look for:

- `_[illegible]parameter`
- `_health_token` parameter
- base64 payloads
- unknown admin access

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

16. Verify Security Plugins

The malware could have disabled or modified the security plugins (e.g. Wordfence).

- Reinstall and re-enable them
- Run a full scan

---

17. Harden the Site

After cleanup:

- Enable 2FA for admins
- Disable PHP execution in uploads folder
- Keep everything updated
- Use strong passwords
- Limit admin access

Summary

- A malicious version (**3.5.1.35**) was briefly distributed
- A fixed version (**3.5.1.36**) is available
- Only **Pro version** is affected
- Infection includes **admin creation, backdoors, and remote execution**
- Use the **cleanup plugin** for easiest recovery
- Manual cleanup is possible but requires careful verification

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!

Final Recommendation

If version **3.5.1.35** was installed:

👉 Treat the site as fully compromised

👉 Perform a full audit

👉 Reset all credentials

If unsure, involve a security professional.

Did this answer your question?

RELATED ARTICLES

Last updated on April 9, 2026

Joomla security advisory: Smart Slider 3 3.5.1.35 compromise (/article/2143-joomla-security-advisory-smart-slider-3-pro-3-5-1-35-compromise)

© Nextendweb 2026. Powered by Help Scout (https://www.helpscout.com/docs-refer/?co=Nextendweb&utm_source=docs&utm_medium=footerlink&utm_campaign=Docs+Branding)

We care about your data, and we'd love to use cookies to make your experience better. Cookie Policy (https://nextendweb.com/privacy-policy/)

Great, I love cookies!