Joomla security advisory: Smart Slider 3 3.5.1.35 compromise

Description

A security breach occurred affecting 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.

Upon discovery, servers were immediately shut down and a full security audit was performed. A clean and safe version **3.5.1.36** has since been released.

The malicious version may:

- create unauthorized administrator users
- install hidden backdoor files
- allow remote code execution on the website

If your website installed version **3.5.1.35**, you must perform a full security audit immediately.

If your site is running **3.5.1.34 or earlier**, there is **no action required**.

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

What the malware may do

The malicious code included in version **3.5.1.35** may:

- Create a hidden administrator account (typically starting with `wpsvc_`)
- Reset passwords for that account to maintain access
- Install additional backdoor files in directories such as `/cache` and `/media`
- Allow attackers to execute arbitrary code remotely
- Send site information and credentials to an external server

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

Required Actions (If You Used Version 3.5.1.35)

🔄 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**
4. Use the available **restore/rollback option** to restore that backup

> ⚠️ *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 credentials (#7-Reset-All-Passwords-nBikP), as the attacker might have accessed them.

If you don't have a backup, then follow these steps carefully to secure your website.

---

1. Update Immediately

Install the fixed version:

➡️ 📄 **Update** (//smartslider.helpscoutdocs.com/article/1752-update#look) **to Smart Slider 3 version 3.5.1.36**

Do not delay this step. If you do not see an update, install Smart Slider again (your sliders will stay!):

- 📄 Joomla 4, 5, 6 (//smartslider.helpscoutdocs.com/article/2043-joomla-4-installation#upload)
- 📄 Joomla 3 (//smartslider.helpscoutdocs.com/article/1759-joomla-installation#upload)

---

2. Put Your Site in Maintenance Mode

Before cleanup:

- E[illegible] maintenance mode, or
- Temporarily restrict access to the site

This prevents further unauthorized access during remediation.

---

3. Create a Full Backup

Before making changes, create a backup of:

- All website files
- The full database

Label this as an **infected backup** for reference.

---

4. Check for Unauthorized Admin Users

Review all administrator accounts in your CMS.

Look for:

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

If found:

- Disable the user immediately
- Then delete it after verification

Also review all admin users and remove anything suspicious.

---

5. Remove Backdoor Files

Check for and delete the following files if present:


```
/ca[illegible]f_check.php
/media/cf_check.php
```

Then search your entire site for suspicious patterns such as:

- `eval(base64_decode`
- `shell_exec`
- `_wpc_k`
- `wpjs1.com`
- `wpsvc_`

Remove or investigate any files containing these.

---

6. Replace Infected Files

Reinstall Smart Slider 3 version 3.5.1.36.

---

7. Reset All Passwords

Assume all credentials may be compromised.

Change:

- Admin user passwords
- Hosting control panel password
- FTP / SFTP / SSH passwords
- Database password
- Email accounts linked to the site

---

8. Review File System for Additional Threats

Inspect commonly abused directories:

- `/cache/`
- `/media/`

- `/tmp/`
- `/images/`

Look for unexpected `.php` files or recently modified files.

---

9. Reinstall Core and Extensions

To ensure full cleanup:

- Reinstall CMS core files from official sources
- Reinstall all plugins and themes
- Remove unused or untrusted extensions

---

10. Check Logs and Access History

Review:

- Server access logs
- Error logs
- Admin login history

Look for:

- Suspicious requests
- Unknown admin logins
- Access to unusual PHP files

---

11. Verify Security Extensions

The malware could have disabled or modified the security extensions

- Reinstall and re-enable them

- Run a full scan

---

12. Apply Security Best Practices

After cleanup:

- Enable two-factor authentication (2FA) for admin users
- Keep all software up to date
- Use strong, unique passwords
- Restrict admin access where possible
- Maintain regular off-site backups

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?

Last updated on April 9, 2026