Managing Your Plugin's Security

- Fixing Security Issues
- Automatic Plugin Security Updates
  - Criteria
- FAQ
  - How do I request my plugin be automatically updated?
  - Can I include changes besides the security related ones for automated updates?
  - Why did plugin A get a automatic update, but plugin B didn't?
  - How can I disable automatic updates?
  - What if I can't (or don't want to) fix my code?
  - Do I only have to fix the reported issue?
  - What if I have guideline issues?

The security of code in WordPress plugins is taken very seriously.

[warning]If you have found a plugin with a security issue, please read Reporting Plugin Security Issues.[/warning]

When a plugin vulnerability is verified by the WordPress Security Team, they contact the plugin author and direct them as to how to fix and release a secure version of the plugin. If there is a lack of response from the plugin author or if the vulnerability is severe, the plugin/theme is pulled from the public directory, and in some cases, fixed and updated directly by the Security Team.

Fixing Security Issues

When you receive a report of security issues in your plugins, it can be terrifying. First, don't panic. Everyone makes mistakes. What matters most is fixing it safely and promptly.

1. Make sure you understand the report. If you're not sure what it means, ask for details. Even third-party reporters are usually willing to take the time to explain what's wrong and direct you where to research a proper fix.
2. Keep your changes as small as possible. This will make it much easier for you to review later on.
3. Test your plugin. Make sure the security fix doesn't break anything else. Make sure upgrading doesn't cause weird errors. Keep `WP_DEBUG` on and log any errors.
4. Document the issue in your change log. You don't need to include details on exactly what happened, but do document that a security issue was resolved.
5. Credit the reporter in your readme. This is just nice, and makes people more inclined to help you for free later on.
6. Bump your version number. We recommend SemVer, so a security release for version 3.9 of your plugin would change the version to 3.9.1 and so on.

Automatic Plugin Security Updates

Since WordPress 3.7, we have had the ability to push automatic security updates for plugins to fix critical vulnerabilities in plugins. Many sites have made use of the plugin automatic updates functionality, either by opting in directly through filters, or by using one of the many remote management services for WordPress that are available.

In extreme situations, the Plugins Team and the WordPress Security Team may determine a plugin issue is great enough that it must be updated for all users. This is exceptionally rare, as the potential for conflicts is high.

The process of approving a plugin for an automatic update, and rolling it out to WordPress users, is highly manual. The security team reviews all code changes in the release, verifies the issue and the fix, and confirms the plugin is safe to trigger an update. Rolling out an automatic update requires modification and deployment of the API code. This is the same standard and process for a core security release.

Criteria

The current criteria we take into consideration for a security push is a simple list:

1. Has the security team been made aware of the issue?
2. How severe is the issue? What impact would it have on the security of a WordPress install, and the greater internet?
3. Is the fix for the issue self-contained or does it add significant extra superfluous code?
4. If multiple branches of the plugin are affected, has a release per branch been prepared?
5. Can the update be *safely* installed automatically?

These requirements are defined in a way that anyone should be able to tick each box.

The first criterion — making the security team aware of the issue — is critical. Since it's a tightly controlled process, the WordPress security team needs to be notified as early as possible. Letting us know is as simple as emailing us at `plugins@wordpress.org` with the details.

The plugin and security teams will work with the plugin author (and the reporter, if different) to study the vulnerability and its exact exposure, verify the proposed fix, and determine what versions will be released and when.

FAQ

How do I request my plugin be automatically updated?

If you feel your plugin has a large enough user base or the issue is of great significance, email `plugin@wordpress.org` **before** you push the code. Include a patch of the changes for review in the email, and explain why you feel this should be automated.

Can I include changes besides the security related ones for automated updates?

With few exceptions, no. A security push should *only* be security related. We prefer (and many times require) plugin releases which fix **only** the security issue, with minimal code changes and with no unrelated changes.

This allows everyone to review the changes quickly and to be far more confident in them. Also it means there is a minimal amount of disruption on the part of the users.

Why did plugin A get a automatic update, but plugin B didn't?

It's not bias from WordPress.org, it's just a throwback to the manual process we've been using. If we're alerted to an issue, we'll work to handle it. If we find out several days later, the window of opportunity to get the fix rolled out has usually passed and it won't be as effective.

How can I disable automatic updates?

There are several options to disable this functionality. The article for disabling core automatic updates applies here. Anything that disables all automatic update functionality will prevent plugin updates. If you only wish to disable plugin updates, whether for all plugins or a single plugin, you can do so with a single filter call.

What if I can't (or don't want to) fix my code?

You don't have to. Your plugin will remain closed and, after 2 or 3 months, the plugin page will report that it was closed for security issues. If you want to push a fix but keep the plugin closed, we can do that too. Just reply to the email and talk to us.

Do I only have to fix the reported issue?

Yes and no. You *do* have to fix the issues reported, but when you're done, the *entire* plugin is re-reviewed, and if more issues are found, you'll be required to fix those as well. The ultimate goal is to make sure the reopened plugin is safe.

What if I have guideline issues?

This comes up when people are breaking other guidelines like including their own copy of jQuery or making undocumented external service calls. It depends on the severity of the other issues. If it's just your own jQuery, we'll likely let it be reopened and allow you to fix that at your own pace. If you're logging all installs of your plugins, you'll be required to correct that before we reopen the plugin.

□□□ #2
□ □□□ □□□ 2026-10-26 07:37:07 UTC
□ □□□ □□□ 2026-10-26 07:37:07 UTC