Installing the Fix for an Exploited WordPress Flaw Can Briefly Expose Some Sites



A researcher at Picus Security reports that some WordPress sites remain open to attack while installing the fix for an actively exploited flaw, because the update runs on the old, unpatched code.

- The flaw is already being exploited in attacks.
- Researcher Umut Bayram of Picus Security found the update-time weakness.
- The update unpacks its files using the site's old, unpatched code.
- An attacker who acts at the right moment can run code on the server.
- The researcher advises blocking web access to certain resources; the source excerpt is cut off before naming them.

A researcher at Picus Security, Umut Bayram, has described a weakness that affects the way a fix is applied for an actively exploited WordPress flaw. According to his findings, installing the patch does not fully close the door at the moment of installation on some sites.

What the researcher found

The update process unpacks its files using the site's existing code, which at that point is still the old, unpatched version. An attacker who strikes at precisely the right moment during the update can therefore run code on the server, even though the site is in the middle of being fixed.

The researcher advises blocking web access to certain items while the update runs. The source text available to us is truncated before it says which ones, so we do not list them here. Check the original report and the vendor's guidance for the exact steps.

What it means for institutions

The practical lesson is that the update window itself carries risk for affected sites. Because the underlying flaw is already being exploited, delaying the update is not a safe option either. The sensible approach is to patch promptly while reducing exposure during the update.

Teams that run WordPress for public portals, customer-facing sites or marketing properties should treat this as a change-management item: schedule the update, restrict access while it runs, and review the site afterwards for signs of tampering.

What to do now

1. Inventory all WordPress sites, including those run by marketing teams or third parties.
2. Read the original report and vendor guidance to identify exactly which web access to block during the update.
3. Schedule the update in a controlled window and restrict web access to the site while it runs.
4. After updating, review the site for unexpected files, new admin accounts and unusual server activity.
5. Record the update in change management and confirm the patched version is in place.