



Recently there were several reports on the following:
**Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update
04/28/2026**

[Sign in](#)

[cPanel](#) > [cPanel & WHM](#) > [Support Topics](#) > [Security](#)

Articles in this section ▼

Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026



Devon Courtney

21 minutes ago · Updated

[Follow](#)

Latest Article Changes:

04/29/26 02:46PM CST: Updated article's required actions and added detection script.

04/28/26 04:36PM CST: Updated article to include patched versions.

04/28/26 03:19PM CST: Updated article to reflect changes in mitigation steps

04/28/26 12:05PM CST: Initial article published.

Cause

An authentication bypass security issue has been identified in the cPanel software (including DNSOnly) affecting all versions after 11.40.

Resolution

We have pushed out a patch for the following cPanel & WHM versions:

- 11.110.0.97
- 11.118.0.63
- 11.126.0.54
- 11.130.0.18
- 11.132.0.29
- 11.136.0.5
- 11.134.0.20

We have pushed out a patch for the following WP Squared version:

- 136.1.7

Required Actions

1. Update the server to one of the above-listed versions immediately via the cPanel update script:

```
/scripts/upcp --force
```

2. Once the update has been completed, verify and confirm the cPanel build version being returned and perform a restart of the cPanel service (cpsrvd):

```
/usr/local/cpanel/cpanel -V
```

```
/scripts/restartsrv_cpsrvd
```

3. Please note that if you have disabled cPanel updates or pinned your cPanel update configuration to a specific version, then these will not auto-update. Please identify and update these servers manually as a priority. Information on how to customize cPanel's Update Preferences from the Command line can be found via the following support article:

[How to customize cPanel's Update Preferences from the Command Line](#)

4. In cases where you are not able to perform the above resolution, please apply one of the following mitigations:

- Block inbound traffic on ports 2083, 2087, 2095, and 2096 at the firewall. **Or,**
- Stop cpsrvd and cpdavd:

```
whmapi1 configureservice service=cpsrvd enabled=0 monitored=0 &&
```

We are currently working on finding paths to get a patch to versions not included above, especially for versions that have higher quantities of servers. In the meantime, it is highly recommended that you follow the instructions below until you can update to a supported version above that will continue to be updated as we release patches.

Warning: If your server is not running a supported version of cPanel that is eligible for this update, it is highly recommended that you work toward updating your server as soon as possible, as it may also be affected.



Was this article helpful?

Yes

No

18 out of 26 found this helpful

Have more questions?

[Submit a Request](#)

[Return to top](#) ^

Related articles

[MySQL8.4 upgraded to MySQL9.7 during nightly updates.](#)

[How to Enable or Disable Service \(Proxy\) Subdomains](#)

[Why is my cPanel AutoSSL \(Powered by Sectigo\) request failing for some domains?](#)

[AutoSSL excludes www for new accounts](#)

LFD is stopped and does not start automatically after cPanel version upgrades

Comments

0 comments

Article is closed for comments.

cPanel