

Alert Bulletin

Bulletin N.: 94

Publication Date: 28/08/2026

Subject: Alert 2026-94 Critical Vulnerability in cPanel /WHM

Traffic Light Protocol (TLP): White

Affected product(s):

cPanel/WHM: all supported versions prior to:

- o 11.110.0.141
- o 11.134.0.53
- o 11.136.0.37
- o 11.138.0.2

WP² (WP Squared):

- o versions prior to 11.138.1.7

Description

On August 27, 2026, cPanel published a security advisory about the vulnerability **CVE-2026-65643**, a critical flaw in the parked domains and addon domains functionality of cPanel/WHM, a widely used administration platform in web hosting services. The vendor has not published a CVSS score; however, it classifies the issue as critical due to the impact of a successful exploitation.

The flaw allows an already authenticated cPanel account holder, with permissions to add parked or addon domains, to create arbitrary files on the server. This capability can be chained to achieve code execution with root privileges, fully compromising the underlying operating system.

As a result, an attacker could gain full control of the server and access or manipulate all hosted accounts, websites, applications, and databases. The vector requires prior authentication, but it represents a particularly high risk in shared hosting or reseller environments, where a low-privilege account could become the entry point to affect multiple customers.

As of August 28, 2026, the vendor has not reported active exploitation, published a PoC, or publicly detailed the exact component or internal mechanism that enables arbitrary write. Neither has a CVE record with official CVSS metrics been published.

Solution:

It is recommended to immediately update cPanel/WHM to the patched version corresponding to the installed branch. The vendor's advisory and patched versions are available at the [official cPanel patch](#).

The update can be performed from WHM, at Home > cPanel > Upgrade to Latest Version, or via SSH with root privileges using:

```
/usr/local/cpanel/scripts/upcp -force
```

Systems running unsupported versions should migrate to a supported branch to receive the fix. As a temporary measure, if updating immediately is not possible, it is advisable to restrict or disable for non-administrative accounts the ability to add parked domains and addon domains, reducing the attack surface until the update is completed.

Additional information:

- <https://support.cpanel.net/hc/en-us/articles/42959571221527-Security-CVE-2026-65643-Vulnerability-in-cPanel-s-Domain-Parking-Functionality-August-27-2026>
- <https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-cpanel-y-whm-permite-escalada-a-root/>
- <https://thehackernews.com/2026/08/critical-cpanel-flaw-could-let-one.html>