



Tanggal 26 Juni 2026

PANDUAN KEAMANAN CVE-2026-41940

DESKRIPSI UMUM

Web defacement melalui cPanel dapat terjadi akibat eksploitasi CVE-2026-41940, sebuah kerentanan authentication bypass kritis pada cPanel & WHM. Kerentanan ini disebabkan oleh CRLF Injection pada daemon cpsrvd yang menulis file sesi ke disk sebelum autentikasi selesai — tanpa sanitasi data. Penyerang menyuntikkan karakter `\r\n` melalui header basic authorization berbahaya untuk menyisipkan properti arbitrer seperti `user=root` ke dalam file sesi, sehingga mendapatkan akses administrator penuh tanpa kredensial valid.

Eksplorasi ini telah dimanfaatkan secara massal untuk meretas server, mendeface website, mengenkripsi data, dan menyebarkan malware — dengan Censys mengidentifikasi 8.859 host terdampak yang terekspos dengan file berekstensi .sorry.

VERSI SISTEM TERDAMPAK

- ▶ cPanel & WHM 11.136.0 — versi sebelum fixed version 11.136.0.5
- ▶ WP Squared — versi sebelum fixed version 136.1.7

9.8
(Critical)

cPanel®

REKOMENDASI

- **Patching:** Memperbarui cPanel & WHM ke versi yang sudah dipatch (minimal 11.136.0.5) dan menjalankan detection script resmi cPanel untuk memindai artefak eksploitasi pada direktori sesi.
- **Security Parameter:** Mengaktifkan EDR/antimalware, menerapkan MFA pada akses WHM dan cPanel, serta membatasi akses port manajemen (2083, 2087) hanya dari IP terpercaya.
- **Review Konfigurasi:** Melakukan segmentasi jaringan, pemantauan aktivitas anomali pada sesi dan log autentikasi, serta isolasi segera server yang terindikasi terinfeksi untuk mencegah penyebaran lateral ke akun hosted lainnya.

SUMBER REFRENSI

- ▶ <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>
- ▶ <https://labs.watchtowr.com/the-internet-is-falling-down-falling-down-falling-down-cpanel-whm-authentication-bypass-cve-2026-41940/>
- ▶ <https://www.cyber.gc.ca/en/alerts-advisories/al26-008-vulnerability-affecting-cpanel-webhost-manager-whm-cve-2026-41940>

