Daily brief, Thursday, April 30, 2026

Apr 29, 8:00 PM to Apr 30, 8:00 PM ET

Generated Nov 7, 2026, 4:22 AM ET

0	1	0	11	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 11 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-41940** WebPros cPanel & WHM and WP2 (WordPress Squared) CISA KEV DETECTION

WebPros cPanel & WHM (WebHost Manager) and WP2 (WordPress Squared) contain an authentication bypass vulnerability in the login flow that allows unauthenticated remote attackers to gain unauthorized access to the control panel.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

11

9.8 **CVE-2026-41940** WebPros cPanel & WHM and WP2 (WordPress S… KEV EXPLOIT CODE DETECTION

WebPros cPanel & WHM (WebHost Manager) and WP2 (WordPress Squared) contain an authentication bypass vulnerability in the login flow that allows unauthenticated remote attackers to gain unauthorized access to the control panel.

9.8 **CVE-2026-4670** Progress moveit automation

Authentication bypass by primary weakness vulnerability in Progress Software MOVEit Automation allows Authentication Bypass. This issue affects MOVEit Automation: from 2025.0.0 before 2025.0.9, from 2024.0.0 before 2024.1.8, versions prior to 2024.0.0.

10.0 **CVE-2026-36767**

A path traversal vulnerability in the /content/images/add endpoint of shopizer v3.2.5 allows attackers write arbitrary files to any writeable path via a crafted POST request.

10.0 **CVE-2026-35051** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is an authentication bypass vulnerability in Traefik's ForwardAuth middleware when trustForwardHeader=false is configured and Traefik is deployed behin

10.0 **CVE-2026-39858** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Prior to versions 2.11.43, 3.6.14, and 3.7.0-rc.2, there is a high severity authentication bypass vulnerability in Traefik's ForwardAuth and snippet-based authentication middleware. Traefik's forwarded-header

9.8 **CVE-2022-50993**

Weaver (Fanwei) E-office versions prior to 10.0_20221201 contain an unauthenticated arbitrary file upload vulnerability in the OfficeServer.php endpoint that allows remote attackers to upload malicious files by sending multipart POST requests with arbitrary fi

9.8 **CVE-2025-71284** Synway smg gateway management software

Synway SMG Gateway Management Software contains an OS command injection vulnerability in the RADIUS configuration endpoint at /en/9-2radius.php where the radius_address POST parameter is split and interpolated directly into a sed command without sanitization.

9.8 **CVE-2026-33446** Absolute secure access

CVE-2026-33446 is a buffer overflow in the authentication sub-system of the Secure Access client prior to 14.50. Attackers with control of a modified server can send a special packet that can overwrite a small portion of memory conceivably leading to memory co

9.8 **CVE-2026-33447** Absolute secure access

CVE-2026-33447 is a buffer overflow in a message parsing function of the Secure Access client prior to 14.50. Attackers with control of a modified server can send a special packet that can overwrite a small portion of memory conceivably leading to memory corru

9.6 **CVE-2026-36760**

An issue in the fileMd5 parameter in the /a/file/upload endpoint of JeeSite v5.15.1 allows authenticated attackers with file upload permissions to execute a path traversal and write arbitrary files with whitelisted suffixes to arbitrary filesystem locations wh

9.1 **CVE-2025-14543** Rti connext professional

Improper Restriction of XML External Entity Reference vulnerability in RTI Connext Professional (Core Libraries) allows Serialized Data External Linking. This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.1, from 6.1.0 be

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.