Daily brief, Sunday, July 12, 2026

Jul 11, 8:00 PM to Jul 12, 8:00 PM ET

Generated Nov 3, 2026, 8:05 PM ET

0	0	0	3	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

3

9.8 **CVE-2026-15511** Comfast CF-WR631AX V3

A vulnerability was determined in Comfast CF-WR631AX V3 up to 2.7.0.8. Affected by this vulnerability is the function system_wl_upload_pic_file of the file /usr/bin/webmgnt of the component FastCGI Backend. This manipulation of the argument filename causes os

9.8 **CVE-2026-56271** Flowiseai flowise

Flowise before 3.1.0 (affected versions 3.0.13 and earlier) uses weak hardcoded default JWT secrets ('auth_token', 'refresh_token') and default audience and issuer values ('AUDIENCE', 'ISSUER') in the enterprise passport authentication middleware (packages/ser

9.1 **CVE-2026-56260** Kidocode crawl4ai

Crawl4AI before 0.8.7 contains an arbitrary file write vulnerability in the Docker API server's /screenshot and /pdf endpoints. The output_path parameter accepts arbitrary filesystem paths without validation, allowing an attacker to supply absolute or path-tra

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. CVE IDs link to the full record on Watch Floor.