Daily brief, Monday, June 8, 2026

Jun 7, 8:00 PM to Jun 8, 8:00 PM ET

Generated Nov 5, 2026, 4:22 AM ET

0	2	0	17	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 17 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.3 **CVE-2026-50751** Check Point Security Gateway CISA KEV DETECTION

An attacker can bypass user authentication and establish a remote access VPN connection without a valid user password on Check Point Security Gateway.

8.7 **CVE-2026-42271** BerriAI LiteLLM CISA KEV DETECTION

An authenticated attacker gains remote code execution on BerriAI LiteLLM.

New public exploit code

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

New critical CVEs 17

9.3 **CVE-2026-50751** Check Point Security Gateway KEV EXPLOIT CODE DETECTION

An attacker can bypass user authentication and establish a remote access VPN connection without a valid user password on Check Point Security Gateway.

9.8 **CVE-2026-25555** EXPLOIT CODE DETECTION

OpenBullet2 through version 0.3.2 contains an authentication bypass vulnerability in the API key authentication middleware that allows unauthenticated attackers to gain admin access by supplying an empty X-Api-Key header value. Attackers can exploit the middle

9.8 **CVE-2026-29167** Apache http server

Use After Free vulnerability in Apache HTTP Server with mod_ldap in per-directory configuration This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.

9.8 **CVE-2026-44631** Apache http server

Buffer Underwrite vulnerability in Apache HTTP Server on crafted regular expressions in the configuration. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.

9.8 **CVE-2026-46289** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: lib/scatterlist: fix length calculations in extract_kvec_to_sg Patch series "Fix bugs in extract_iter_to_sg()", v3. Fix bugs in the kvec and user variants of extract_iter_to_sg. This series is

9.1 **CVE-2026-42535** Apache http server

A path handling issue in mod_dav_fs in Apache 2.4.67 and earlier allows a WebDAV content author to directly manipulate trusted DAV property databases, potentially causing child process crashes. Users are recommended to upgrade to version 2.4.68, which fixes th

9.9 **CVE-2026-46442** Flowiseai flowise DETECTION

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, POST /api/v1/node-custom-function lacks route-level authorization, allowing any authenticated user or API key to submit arbitrary JavaScript to the

9.8 **CVE-2023-54352**

WordPress Seotheme contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by uploading malicious files to the theme directory. Attackers can access the uploaded PHP shell at /wp-content/themes/seothem

9.8 **CVE-2024-58348**

WordPress Background Image Cropper version 1.2 contains a remote code execution vulnerability that allows unauthenticated attackers to upload arbitrary files by accessing the ups.php endpoint. Attackers can upload PHP files through the file upload form in the

9.8 **CVE-2024-58349**

WordPress Theme Travelscape 1.0.3 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by exploiting insufficient validation in the theme's upload functionality. Attackers can upload arbitrary files to

9.8 **CVE-2026-11499** DETECTION

A vulnerability was determined in Tenda HG7, HG9 and HG10 300001138_en_xpon. This affects the function formDOMAINBLK of the file /boaform/formDOMAINBLK. Executing a manipulation of the argument blkDomain can lead to stack-based buffer overflow. The attack may

9.8 **CVE-2026-52778**

YesWiki is a wiki system written in PHP. Prior to version 4.6.6, an unsafe execution vulnerability exists in the Bazar form field calculator (CalcField.php) of YesWiki. The application attempts to sanitize user-defined mathematical formulas using a complex rec

9.6 **CVE-2026-42861** Flowiseai flowise

+1 more CVEs in the same release

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, a mass assignment vulnerability exists in the variable update endpoint of FlowiseAI. The endpoint allows authenticated users to modify server-contr

9.4 **CVE-2026-41448**

AdGuard Home, when started with the --glinet flag, contains an authentication bypass vulnerability that allows unauthenticated attackers to gain full admin access by supplying a path traversal sequence in the Admin-Token cookie, exploiting unsanitized string c

9.1 **CVE-2026-46440** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, the checkBasicAuth endpoint validates credentials in plaintext without rate limiting and with direct comparison. This issue has been patched in ver

9.0 **CVE-2026-11393**

Improper neutralization of triple-quote characters during Python code generation in AgentCore CLI before v0.14.2 might allow an authenticated remote threat actor to execute arbitrary code on AWS AgentCore Runtime under the imported agent's IAM execution role a

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.