Daily brief, Monday, August 10, 2026

Aug 9, 8:00 PM to Aug 10, 8:00 PM ET

Generated Nov 2, 2026, 4:51 PM ET

0	0	0	84	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

84 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

84

9.9 **CVE-2026-72911** Frappe erpnext

ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.118.0 and 16.29.0, the validate_template and render_template calls in erpnext/accounts/doctype/process_statement_of_accounts/process_statement_of_accounts.py render subject, body,

9.3 **CVE-2026-48160** Dai-Shi react-tracked

react-tracked provides state usage tracking with Proxies. Between 2026-05-18 19:26:36 and 2026-05-19 15:22:45, the default branch contained malicious commits 6978272a7d6ca02225cb747ea69f427512e33699 through 949f1a3d6bb1ff7d1a0dec892afd773e742627e8 that execute

9.3 **CVE-2026-48161** Dai-Shi react18-use

react18-use is a React 19 use hook shim. Between 2026-05-19 01:07:01 and 2026-05-19 15:20:43, the default branch contained malicious commits 7b79148d1495a2505f9277da295a98cf176f4496 through 7b79148d1495a2505f9277da295a98cf176f4496 that executed remote attacker

10.0 **CVE-2026-66915**

Joomla Extension - fabrikar.com - Remote code execution in Fabrik < 4.7.2 - An unauthenticated attacker could execute arbitrary code by using the ajax_calc feature of the calc plugin.

10.0 **CVE-2026-72899**

Metabase allows an unauthenticated attacker to inject arbitrary SQL via a publicly shared card or dashboard that exposes a field-filter (dimension) parameter.

9.9 **CVE-2026-72733**

+1 more CVEs in the same release

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the backup.restoreBackupWithLogs tRPC subscription builds database restore shell pipelines from the user-controlled databaseName and backupFile fields without safely separating th

9.9 **CVE-2026-72735**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, writeTraefikConfigRemote in packages/server/src/utils/traefik/application.ts serializes user-controlled Traefik configuration with yaml.stringify and interpolates the resulting ya

9.9 **CVE-2026-72736**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy passes user-controlled values directly into shell commands via unquoted template literal interpolation in the registry credential testing and Docker Swarm cluster manageme

9.9 **CVE-2026-72738**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the backup.listBackupFiles tRPC endpoint in apps/dokploy/server/api/routers/backup.ts passes the search parameter through normalizeS3Path and interpolates it into an rclone lsjson

9.9 **CVE-2026-72740**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, packages/server/src/utils/providers/git.ts parses the user-controlled customGitUrl with sanitizeRepoPathSSH and interpolates its domain into the ssh-keyscan command from addHostTo

9.9 **CVE-2026-72862**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the mariadb.ts, mongo.ts, mysql.ts, postgres.ts, redis.ts, and libsql.ts Dokploy database service deployment functions pass user-controlled dockerImage fields unquoted into docker

9.9 **CVE-2026-72863**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy's WebSocket handlers (in-app terminals and log streamers) authenticate the session but never authorize it. They establish who the user is via validateRequest() and then pr

9.9 **CVE-2026-72864**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the local branch of /docker-container-terminal in apps/dokploy/server/wss/docker-container-terminal.ts authenticates with validateRequest but does not authorize the attacker-contr

9.9 **CVE-2026-72865**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the compose.update operation stores an unvalidated composePath that packages/server/src/utils/builders/compose.ts and packages/server/src/services/compose.ts interpolate into dock

9.9 **CVE-2026-72867** DETECTION

Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.29.3 until 0.29.13, the incomplete fix for CVE-2026-45628 leaves packages/server/src/db/schema/compose.ts branch fields without server-side validation, allowing a direct compose.update reque

9.9 **CVE-2026-72868**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, apps/dokploy/server/api/routers/destination.ts interpolates the accessKey, secretAccessKey, region, endpoint, provider, and bucket fields from destination.testConnection into an r

9.9 **CVE-2026-72872**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, application.saveBitbucketProvider stores bitbucketOwner and bitbucketRepository without validation and cloneBitbucketRepository in packages/server/src/utils/providers/bitbucket.ts

9.9 **CVE-2026-72876**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, swarm.getNodes, swarm.getNodeInfo, swarm.getNodeApps, and swarm.getAppInfos in apps/dokploy/server/api/routers/swarm.ts accept another organization’s serverId without an activeOrg

9.9 **CVE-2026-72880**

Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the apiCreateCertificate schema in packages/server/src/db/schema/certificate.ts accepts a client-supplied certificatePath, and packages/server/src/services/certificate.ts joins th

9.9 **CVE-2026-72882**

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.28.8 and earlier, an authenticated user who can create or update file mounts for a service can inject shell metacharacters into filePath, causing Dokploy to execute attacker-controlled command

63 more critical CVEs in this window: see the dashboard

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.