Daily brief, Thursday, August 13, 2026

Aug 12, 8:00 PM to Aug 13, 8:00 PM ET

Generated Nov 2, 2026, 1:55 PM ET

0	0	0	68	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

68 new critical CVEs, 1 new breaches.

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

68

9.8 **CVE-2026-73487** Flowiseai flowise

Flowise before 3.1.3 contains a regex-based Python code validator bypass in CSV and Airtable Agent nodes that allows unauthenticated attackers to inject malicious code via prompt injection. Attackers can exploit unblocked pandas functions like pd.read_json() t

9.8 **CVE-2026-49827** SMEWebify WebErpMesv2

WebErpMesv2 is a Resource Management and Manufacturing execution system Web for industry. Versions 1.19 and prior allow any self-registered user to upload arbitrary PHP files through the HR Expense scan_file parameter, leading to Remote Code Execution. Combine

10.0 **CVE-2026-27544** QuarkA QA Analytics

Unauthenticated Remote Code Execution (RCE) in QA Analytics <= 5.2.0.0 versions.

9.9 **CVE-2026-73602** Flowiseai flowise

Flowise before 3.1.3 contains a sandbox escape vulnerability in the vm2 JavaScript sandbox that allows authenticated users to execute arbitrary code by exploiting moment locale validation bypass. Attackers can craft a fake String object with a match function t

9.8 **CVE-2026-28008** miniOrange OAuth Single Sign On – SSO (OAuth Client)
Unauthenticated Broken Authentication in OAuth Single Sign On – SSO (OAuth Client) <= 7.0.0 versions.

9.8 **CVE-2026-28149** miniOrange Headless Single Sign On
Unauthenticated PHP Object Injection in Headless Single Sign On <= 1.6 versions.

9.3 **CVE-2026-28001** WPDirectoryKit WP Directory Kit
Unauthenticated SQL Injection in WP Directory Kit <= 1.5.4 versions.

9.3 **CVE-2026-28142** Shamalli Web Directory Free
Unauthenticated SQL Injection in Web Directory Free <= 1.7.13 versions.

9.8 **CVE-2026-28148** miniOrange Headless Single Sign On
Unauthenticated Bypass Vulnerability in Headless Single Sign On <= 1.6 versions.

10.0 **CVE-2026-15413**
The Link Factory WordPress plugin is a backdoor. Distributed as a "homepage sentence publisher", it exposes an operator-controlled REST API under /wp-json/link-factory/v1/ - authenticated by a detached Ed25519 signature verified against a hardcoded operator pu

10.0 **CVE-2026-59500**
: Improper Authentication vulnerability in Priority Portal Generator addon to Priority ERP (developed by Soft Solutions). This issue affects Portal Generator addon to Priority ERP (developed by Soft Solutions): All versions without Priwall v3.

10.0 **CVE-2026-61962**
Unauthenticated Arbitrary Code Execution in WP BASE Booking <= 6.3.0 versions.

10.0 **CVE-2026-72851**
Budibase before 3.40.0 contains an unauthenticated SQL injection vulnerability in webhook-triggered automations with EXECUTE_QUERY steps. Attackers can POST attacker-controlled JSON to the webhook trigger endpoint to inject SQL payloads that execute with build

9.9 **CVE-2026-73656**
Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. Prior to 4.5.6, POST /api/v1/deployments/:deploymentId/background-workers calls CreateDeploymentBackgroundWorkerServiceV4.call() in apps/webapp/app/v3/services/createDe

9.9 **CVE-2026-72841**
luci-app-openvpn fails to properly validate the instance_name2 parameter during file upload, allowing authenticated users to perform path traversal and write arbitrary files outside the intended directory. Attackers can upload malicious payloads to gain persis

9.9 **CVE-2026-72842**
luci-app-lxc contains an ACL inconsistency vulnerability that allows low-privileged authenticated LuCI users to access backend container management routes without proper authorization checks. Attackers can exploit path traversal via `/.%2E` in the `lxc_name` p

9.8 **CVE-2026-16770**

PDF::WebKit versions through 1.2 for Perl allow argument injection into wkhtmltopdf via meta tags in the source document. For an HTML string or file source, the constructor collects every <meta name="pdf-webkit-KEY" content="VALUE"> element in the document hea

9.8 **CVE-2026-49819**

UpSnap is a wake on lan web app. Versions 4.4.1 through 5.3.5 are vulnerable to a missing-authentication / privilege-escalation chain in `pb.HandlerInitSuperuser` (`backend/pb/handlers.go:249`), reachable as `POST /api/upsnap/init-superuser`. The vulnerable co

9.8 **CVE-2026-14182**

The Customer Email Verification for WooCommerce WordPress plugin before 3.2.6 does not correctly validate the email-verification activation code, relying on a loose comparison that an attacker can satisfy with a crafted value type, allowing unauthenticated use

9.8 **CVE-2026-28185**

Unauthenticated Broken Authentication in Log in with Google <= 1.4.2 versions.

48 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

RingCentral ringcentral.com 1,596,490 accounts

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.