Daily brief, Tuesday, June 23, 2026

Jun 22, 8:00 PM to Jun 23, 8:00 PM ET

Generated Nov 4, 2026, 2:01 PM ET

0	4	0	32	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 32 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

10.0 **CVE-2026-34908** Ubiquiti UniFi OS CISA KEV DETECTION
A malicious actor can make unauthorized changes to a Ubiquiti UniFi OS system.

10.0 **CVE-2026-34909** Ubiquiti UniFi OS CISA KEV DETECTION
An attacker can execute code and access arbitrary files on a Ubiquiti UniFi OS server.

10.0 **CVE-2026-34910** Ubiquiti UniFi OS CISA KEV DETECTION
A malicious actor can inject commands on a Ubiquiti UniFi OS server with network access.

9.8 **CVE-2025-67038** Lantronix EDS5000 CISA KEV
An attacker injects arbitrary OS commands into the username parameter with Lantronix EDS5000.

New public exploit code

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

New critical CVEs

32

10.0 **CVE-2026-34910** Ubiquiti UniFi OS KEV EXPLOIT CODE DETECTION
A malicious actor can inject commands on a Ubiquiti UniFi OS server with network access.

10.0 **CVE-2026-34908** Ubiquiti UniFi OS KEV EXPLOIT CODE DETECTION
A malicious actor can make unauthorized changes to a Ubiquiti UniFi OS system.

10.0 **CVE-2026-34909** Ubiquiti UniFi OS KEV EXPLOIT CODE DETECTION

An attacker can execute code and access arbitrary files on a Ubiquiti UniFi OS server.

9.8 **CVE-2025-67038** Lantronix EDS5000 KEV EXPLOIT CODE

An attacker injects arbitrary OS commands into the username parameter with Lantronix EDS5000.

10.0 **CVE-2026-27604** DETECTION

FOSSBilling is a free, open-source billing and client management system. Starting in version 0.5.4 and prior to version 0.8.0, an authorization bypass in the API role handling allows unauthenticated access to privileged `/api/system/*` endpoints. Because `syst

10.0 **CVE-2026-54309** N8n n8n

n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, when @n8n/mcp-browser is run in HTTP transport mode, the MCP endpoint accepts session initialization and tool invocation requests without any authentication. Any network-reachable

10.0 **CVE-2026-48020** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.48, 3.6.19, and 3.7.3, there is a high severity vulnerability in Traefik's StripPrefix middleware that allows an unauthenticated attacker to bypass route-level authentication and authorization.

10.0 **CVE-2026-48491** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. From 3.7.0 until 3.7.3, there is a high severity vulnerability in Traefik's domain-fronting protection (SNICheck) that allows an unauthenticated client to bypass mutual TLS enforced through wildcard router TL

10.0 **CVE-2026-53622** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Versions prior to 3.7.3, 3.6.18, and 2.11.51 have a critical vulnerability in Traefik's HTTP/3 (QUIC) TLS configuration selection that allows unauthenticated clients to bypass router-specific mTLS enforcement

9.9 **CVE-2026-56274** Flowiseai flowise

Flowise before 3.1.2 contains multiple OS command injection vulnerabilities in the Custom MCP Server feature due to incomplete command-flag validation and a regex bypass in local file access restrictions. An attacker with a Flowise account of any role, or API

9.9 **CVE-2026-54310** N8n n8n

n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, an authenticated user with permission to create or modify workflows could supply a crafted parameters to the TimescaleDB and/or legacy Postgres v1 node's allowing arbitrary SQL to

9.9 **CVE-2026-44789** N8n n8n

+1 more CVEs in the same release

n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, an authenticated user with permission to create or modify workflows could achieve global prototype pollution via an unvalidated pagination parameter in the HTTP Request

9.9 **CVE-2026-54305** N8n n8n

n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, three EE endpoints used by the Dynamic Credentials feature accepted any authenticated n8n session without performing per-resource ownership or scope checks on the target

9.8 **CVE-2026-12866**

All versions of the package expr-eval are vulnerable to Code Execution via the toJSFunction() API. An attacker can execute arbitrary JavaScript by supplying crafted expressions that are compiled into native code using new Function(). Because user-controlled ex

9.8 **CVE-2026-56315**

picklescan before 1.0.4 fails to block at least seven Python standard library modules (including uuid, _osx_support, _aix_support, _pyrepl.pager, and imaplib) exposing eight functions that provide direct arbitrary command execution. Attackers can craft malicio

9.8 **CVE-2026-53753** Kidocode crawl4ai DETECTION

Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.7, the _safe_eval_expression() function in the computed fields feature uses an AST validator that only blocks attributes starting with underscore. Python generator and frame object att

9.6 **CVE-2026-48519** Langflow langflow

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, the "Shareable Playground" (or "Public Flows" in code) contains a critical RCE vulnerability. Shareable Playground feature works by enabling the execution of workflo

9.6 **CVE-2026-54307** N8n n8n

n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, a member-level user with editor access to a shared workflow could reference credentials they do not own via specific public API endpoints. Credential ownership checks we

9.6 **CVE-2026-55447** Langflow langflow

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, by controlling a files that are digested into the RAG, an attacker can direct the node to read any file on the file-system by absolute path. All components based on

9.6 **CVE-2026-53662**

immich is a high performance self-hosted photo and video management solution. From commit 4ffa26c9 until 4eb1003, a reflected cross-site scripting (XSS) vulnerability on the /auth/login page allows an attacker to fully compromise any authenticated user's accou

11 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.