Daily brief, Wednesday, July 15, 2026

Jul 14, 8:00 PM to Jul 15, 8:00 PM ET

Generated Nov 3, 2026, 5:37 PM ET

0	2	0	34	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 34 new critical CVEs, 2 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.8 **CVE-2026-46817** Oracle E-Business Suite CISA KEV

An unauthenticated attacker gains takeover of Oracle Payments with Oracle E-Business Suite.

7.5 **CVE-2023-4346** KNX Association KNX Protocol Connection Authorization Option 1 CISA KEV

An attacker can purge all devices without additional security options enabled.

New public exploit code

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

New critical CVEs 34

9.8 **CVE-2026-46817** Oracle E-Business Suite KEV EXPLOIT CODE

An unauthenticated attacker gains takeover of Oracle Payments with Oracle E-Business Suite.

10.0 **CVE-2026-50148** Metabase metabase

Metabase is an open-source business intelligence and embedded analytics tool. From 1.54.0 until 1.54.24, 1.55.24, 1.56.25, 1.57.19, 1.58.14, 1.59.10, and 1.60.4, a Metabase user with permission to add or edit a database connection can achieve remote code execu

10.0 **CVE-2026-46339** DETECTION

9Router is an AI router & token saver. From 0.4.30 until 0.4.37, 9Router's src/proxy.js middleware did not protect /api/cli-tools/* and /api/mcp/*, allowing unauthenticated registration of customPlugins through src/app/api/cli-tools/cowork-settings/route.js an

10.0 **CVE-2026-52887**

NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to 2.0.61, NocoBase @nocobase/plugin-notification-in-app-message exposed GET /api/myInAppChannels:list, where the filter[latestMsgReceiveTime

9.9 **CVE-2026-44986**

Penpot is an open-source design tool for design and code collaboration. Prior to 2.14.5, Penpot exposed teams_invitations.clj invitation tokens from create-team-invitations, embedded an existing profile id in auth.clj prepare-register-profile, and had auth.clj

9.9 **CVE-2026-54052** N8n-Mcp n8n-mcp

n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Prior to 2.56.1, in HTTP mode with multi-tenancy enabled through ENABLE_MULTI_TENANT=true, n8n-mcp's local workflow version history backups were

9.9 **CVE-2026-52891**

Wekan is open source kanban built with Meteor. Prior to 9.07, Wekan avatar upload functionality embeds user-supplied filenames into paths later passed to child_process.exec() for MIME-type detection. Because models/avatars.js and models/fileValidation.js used

9.8 **CVE-2026-14960**

Pegatron `Tdelo64.sys` improperly exposes privileged hardware access functionality through the `\\.\TdeIo` device interface. IOCTL handlers including `TDE_IOCTL_INDEXIO_READ` and `TDE_IOCTL_INDEXIO_WRITE` permit unprivileged user-mode callers to perform arbitr

9.8 **CVE-2026-49352**

9Router is an AI router & token saver. From 0.2.21 until 0.4.44, 9Router used the hardcoded fallback JWT secret 9router-default-secret-change-me in src/app/api/auth/login/route.js, src/middleware.js, and later src/lib/auth/dashboardSession.js, allowing attacke

9.8 **CVE-2026-51380**

Buffer Overflow vulnerability in Tenda AC10 v3 (firmware V03.03.16.09) allows attackers to cause a permanent Denial of Service (DoS) or potentially execute remote code via the /cgi-bin/UploadCfg endpoint

9.8 **CVE-2025-65720**

An issue in Open Source GPT Researcher v3.3.7 allows attackers to execute arbitrary commands on a victim system via user interaction with a crafted HTML page.

9.8 **CVE-2026-30618**

xszyou Fay 4.3.1 contains a remote code execution vulnerability in its MCP STDIO server management and command execution handling. A remote attacker can access the publicly exposed MCP management interface and configure an MCP STDIO server with attacker-contro

9.8 **CVE-2026-30623** DETECTION

LiteLLM 1.18.10 contains a remote code execution vulnerability in its MCP server creation functionality. The application allows users to add MCP servers via a JSON configuration specifying arbitrary command and args values. LiteLLM executes these values on the

9.8 **CVE-2026-55652**

Wekan is open source kanban built with Meteor. Prior to 9.46, header-login with HEADER_LOGIN_TRUSTED_IPS uses getRequestIp() in server/lib/headerLoginAuth.js to trust the client-supplied X-Forwarded-For header before the real socket address, allowing an unauth

9.6 **CVE-2026-61451**

The Grav API plugin (grav-plugin-api) before 1.0.4 does not validate the origin of the client-supplied admin_base_url field in the POST /api/v1/auth/forgot-password endpoint. The sanitizeHttpUrl() function only checks that the URL scheme is http/https and neve

9.6 **CVE-2026-53513** Better-Auth better-auth\/sso

Better Auth is an authentication and authorization library for TypeScript. Prior to 1.6.11, the @better-auth/sso plugin's POST /sso/register and POST /sso/update-provider endpoints accept attacker-controlled oidcConfig.userInfoEndpoint, tokenEndpoint, and jwks

9.6 **CVE-2026-62948** Openwrt openwrt

OpenWrt is a Linux operating system targeting embedded devices. Prior to 25.12.5, odhcpd writes a DHCPv6 client FQDN option 39 hostname into /tmp/odhcpd.leases through src/statefiles.c statefiles_write_state6() and statefiles_write_state4() without escaping, a

9.6 **CVE-2026-54458**

WWBN AVideo is an open source video platform. Versions prior to 29.0 contain a stored DOM Cross-Site Scripting vulnerability in the YPTSocket plugin. Any unauthenticated remote attacker can execute arbitrary JavaScript in the authenticated origin of every admi

9.5 **CVE-2026-13385**

An Improper Validation of Integrity Check Value and Improper Certificate Validation in certain ASUS router models allows a remote man-in-the-middle(MITM) user to make the router download and execute arbitrary command via a spoofed server. Refer to the ' Securi

9.5 **CVE-2026-46684**

DataEase is an open source data visualization and analysis tool. Prior to 2.10.23, DataEase enterprise token handling can let TokenFilter#doFilter() pass X-DE-TOKEN values to TokenUtils.validate(), which checks only token presence and length before userBOByTok

14 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 2

Goose Creek goosecreek.com 6,574,121 accounts

Fluke fluke.com 821,100 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.