Daily brief, Tuesday, June 2, 2026

Jun 1, 8:00 PM to Jun 2, 8:00 PM ET

Generated Nov 5, 2026, 10:05 AM ET

0	2	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 15 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

8.4 **CVE-2025-48595** Android Framework CISA KEV

An attacker gains local privilege escalation in Android Framework.

7.8 **CVE-2022-0492** Linux Kernel CISA KEV

A privilege escalation occurs via the cgroups v1 release_agent feature in the Linux Kernel due to improper authentication.

New public exploit code

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

New critical CVEs 15

10.0 **CVE-2026-10611** Misp-Project misp

An authentication bypass vulnerability exists in MISP when LDAP mixed authentication is enabled with OTP enforcement. In deployments configured with LdapAuth.mixedAuth=true and Security.require_otp=true, users authenticated through an authentication plugin, su

10.0 **CVE-2026-7312** Progress sitefinity

CWE?522: Insufficiently Protected Credentials in web services in Progress Sitefinity version from 14.0.7700 to 14.4.8152, and 15.0.8200 to 15.0.8234, and 15.1.8300 to 15.1.8335, 15.2.8400 to 15.2.8441, 15.3.8500 to 15.3.8531, and 15.4.8600 to 15.4.8630 allows

9.8 **CVE-2026-8206**

The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions 6.0.0 to 6.0.6. This is due to the plugin accepting an arbitrary email address when a username is us

9.8 **CVE-2025-53209**

Incorrect Privilege Assignment vulnerability in Themeisle Masteriyo LMS PRO allows Privilege Escalation. This issue affects Masteriyo LMS PRO: from n/a through 2.20.0.

9.8 **CVE-2026-7198** Progress sitefinity

CWE-284: Improper Access Control in web services in Progress Sitefinity 15.4.8623 before 15.4.8630 allows a remote unauthenticated attacker to access content that should be restricted, resulting in full compromise of confidentiality, integrity, and availabilit

9.8 **CVE-2026-47117**

OpenMed before 1.5.2 contains a remote code execution vulnerability in the PII privacy-filter model loading path. The privacy-filter dispatcher used broad substring matching on the user-supplied model_name parameter, allowing a value such as attacker/foo-priva

9.8 **CVE-2026-0611**

Spacelabs Healthcare Sentinel versions 10.5.x and higher and 11.x.x before 11.6.0 contain an unauthenticated remote code execution vulnerability through a deprecated .NET Remoting HTTP channel exposed on port 8989 that allows attackers to perform arbitrary fil

9.8 **CVE-2026-42074** Gitlawb openclaude

OpenClaude is an open-source coding-agent command line interface for cloud and local model providers. Prior to version 0.5.1, the dangerouslyDisableSandbox parameter is exposed as part of the BashTool input schema, meaning the LLM (an untrusted principal per t

9.8 **CVE-2026-38967**

CrowCpp Crow through v1.3.1 HTTP is vulnerable to response header injection via unvalidated response header values.

9.8 **CVE-2026-5076**

The ARMember Premium plugin for WordPress is vulnerable to an insecure password reset mechanism in all versions up to, and including, 7.3.1. The plugin stores a plaintext copy of the password reset key in the `arm_reset_password_key` user meta field when a use

9.8 **CVE-2026-49448** Goauthentik authentik

authentik is an open-source identity provider. Prior to versions 2025.12.6, 2026.2.4, and 2026.5.1, the Source stage can be bypassed by sending an empty POST. This issue has been patched in versions 2025.12.6, 2026.2.4, and 2026.5.1.

9.6 **CVE-2026-32625** Librechat librechat

LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. In versions up to and including 0.8.3, the Model Context Protocol (MCP) server integration resolves ${VAR} placeholders against the server's process.env during Zod schema validation of

9.3 **CVE-2026-34906**

Server-Side Template Injection (SSTI) in Wirtualna Uczelnia allows an unauthenticated attacker to perform Remote Code Execution (RCE). In the endpoint redirectToUrl and parameter redirectUrlParameter, insufficient input validation permits injection of arbitrar

9.3 **CVE-2026-42684**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ahmad WP Job Portal allows Blind SQL Injection. This issue affects WP Job Portal: from n/a through 2.5.1.

9.3 **CVE-2026-42849** Goauthentik authentik

authentik is an open-source identity provider. Prior to versions 2025.12.5 and 2026.2.3, due to the implementation of stages in the SFE (Simple Flow Executor) in order to make the interface more compatible with legacy browsers, it was possible to use an XSS ex

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.