Daily brief, Thursday, April 16, 2026

Apr 15, 8:00 PM to Apr 16, 8:00 PM ET

Generated Nov 7, 2026, 6:51 AM ET

0	1	0	18	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 18 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2026-34197** Apache ActiveMQ CISA KEV DETECTION

Improper input validation in Apache ActiveMQ allows an attacker to inject code, resulting in code execution on the affected ActiveMQ server.

New public exploit code

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

New critical CVEs

18

9.8 **CVE-2026-27820** Ruby-Lang zlib

zlib is a Ruby interface for the zlib compression/decompression library. Versions 3.0.0 and below, 3.1.0, 3.1.1, 3.2.0 and 3.2.1 contain a buffer overflow vulnerability in the Zlib::GzipReader. The zstream_buffer_ungets function prepends caller-provided bytes

9.8 **CVE-2026-4880**

The Barcode Scanner (+Mobile App) – Inventory manager, Order fulfillment system, POS (Point of Sale) plugin for WordPress is vulnerable to privilege escalation via insecure token-based authentication in all versions up to, and including, 1.11.0. This is due to

9.8 **CVE-2026-40504**

Creolabs Gravity before 0.9.6 contains a heap buffer overflow vulnerability in the gravity_vm_exec function that allows attackers to write out-of-bounds memory by crafting scripts with many string literals at global scope. Attackers can exploit insufficient bo

9.8 **CVE-2026-6349**

The iSherlock developed by HGiga has an OS Command Injection vulnerability, allowing unauthenticated local attackers to inject arbitrary OS commands and execute them on the server.

9.8 **CVE-2026-6350**

MailGates/MailAudit developed by Openfind has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and execute arbitrary code.

9.8 **CVE-2026-3596**

The Riaxe Product Customizer plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.1.2. The plugin registers an unauthenticated AJAX action ('wp_ajax_nopriv_install-imprint') that maps to the ink_pd_add_option() fun

9.8 **CVE-2026-31843**

The goodoneuz/pay-uz Laravel package (<= 2.2.24) contains a critical vulnerability in the /payment/api/editable/update endpoint that allows unauthenticated attackers to overwrite existing PHP payment hook files. The endpoint is exposed via Route::any without a

9.8 **CVE-2026-37339**

SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_genre.php.

9.8 **CVE-2026-37340**

SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/edit_music.php.

9.8 **CVE-2026-37345**

SourceCodester Vehicle Parking Area Management System v1.0 is vulnerable to SQL Injection in the file /parking/manage_park.php.

9.8 **CVE-2026-33082** Dataease dataease

DataEase is an open source data visualization analysis tool. Versions 2.10.20 and below contain a SQL injection vulnerability in the dataset export functionality. The expressionTree parameter in POST /de2api/datasetTree/exportDataset is deserialized into a fil

9.8 **CVE-2026-33122** Dataease dataease

DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the API datasource update process. When a new table definition is added during a datasource update via /de2api/datasource/

9.4 **CVE-2026-37338**

SourceCodester Simple Music Cloud Community System v1.0 is vulnerable to SQL Injection in the file /music/view_user.php.

9.3 **CVE-2026-40959**

Luanti 5 before 5.15.2, when LuaJIT is used, allows a Lua sandbox escape via a crafted mod.

9.1 **CVE-2026-6270** Fastify fastify\/middie

@fastify/middie versions 9.3.1 and earlier do not register inherited middleware directly on child plugin engine instances. When a Fastify application registers authentication middleware in a parent scope and then registers child plugins with @fastify/middie, t

9.1 **CVE-2026-37347**

SourceCodester Payroll Management and Information System v1.0 is vulnerable to SQL Injection in the file /payroll/view_employee.php.

9.1 **CVE-2026-5426**

Hard-coded ASP.NET/IIS machineKey value in Digital Knowledge KnowledgeDeliver deployments prior to February 24, 2026 allows adversaries to circumvent ViewState validation mechanisms and achieve remote code execution via malicious ViewState deserialization atta

9.0 **CVE-2026-40322** B3log siyuan

SiYuan is an open-source personal knowledge management system. In versions 3.6.3 and below, Mermaid diagrams are rendered with securityLevel set to "loose", and the resulting SVG is injected into the DOM via innerHTML. This allows attacker-controlled javascrip

Ransomware

No leak-site posts collected.

New data breaches 1

McGraw Hill mheducation.com 13,500,136 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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.