Daily brief, Monday, May 18, 2026

May 17, 8:00 PM to May 18, 8:00 PM ET

Generated Nov 7, 2026, 12:46 AM ET

0	0	0	14	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

14 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

14

10.0 **CVE-2026-45829** Chroma ChromaDB EXPLOIT CODE

A pre-authentication, code injection vulnerability in version 1.0.0 or later of the ChromaDB Python project allows an unauthenticated attacker to run arbitrary code on the server by sending a malicious model repository and trust_remote_code set to true in the

10.0 **CVE-2026-42822** Microsoft azure local

Improper authentication in Azure Local Disconnected Operations allows an unauthorized attacker to elevate privileges over a network.

9.1 **CVE-2026-45230** DumbWareio DumbAssets

DumbAssets through 1.0.11 contains a path traversal vulnerability in the POST /api/delete-file endpoint and filesToDelete array parameters that allows unauthenticated attackers to delete arbitrary files by supplying ../ sequences that bypass directory boundary

9.3 **CVE-2026-4320** Creartia Internet Consulting ICMS Content Management

Authorization Bypass vulnerability in Creartia's ICMS software could allow an attacker to gain unauthorized access to protected features by manipulating the HTTP redirect headers of the login process, causing the script to continue running and enabling privile

9.9 **CVE-2026-27130**
Dokploy is a free, self-hostable Platform as a Service (PaaS). Versions 0.26.6 and below have OS command injection through the appName parameter. 3 chained issues cause this problem: inadequate input sanitization, lack of schema validation and direct shell int

9.8 **CVE-2026-7301** Lmsys sglang
SGLangs multimodal generation runtime scheduler's ROUTER socket binds to 0.0.0.0 by default and contains a sink that calls pickle.loads() on incoming messages, enabling RCE when exposed to the internet.

9.8 **CVE-2026-7304** Lmsys sglang
SGLangs multimodal generation runtime is vulnerable to unauthenticated remote code execution when the --enable-custom-logit-processor option is enabled, as Python objects loaded via dill.loads() will be deserialized without validation.

9.8 **CVE-2026-8836**
A vulnerability was found in lwIP up to 2.2.1. Affected is the function snmp_parse_inbound_frame of the file src/apps/snmp/snmp_msg.c of the component snmpv3 USM Handler. Performing a manipulation of the argument msgAuthenticationParameters results in stack-ba

9.8 **CVE-2026-25244** Openjsf webdriverio
WebdriverIO is a test automation framework for unit, e2e and component testing using WebDriver, WebDriver BiDi and Appium. Versions below 9.24.0 contain a command injection vulnerability leading to remote code execution (RCE) in test orchestration. Git permits

9.8 **CVE-2026-8838**
Unsafe use of Python's eval() on server-received data in the vector_in() function in amazon-redshift-python-driver before 2.1.14 allows a rogue server or man-in-the-middle actor to execute arbitrary code on the client. To remediate this issue, users should upg

9.4 **CVE-2026-41948** Dify dify DETECTION
Dify version 1.14.1 and prior contain a path traversal vulnerability that allows authenticated users to manipulate requests forwarded to the Plugin Daemon's internal REST API by exploiting insufficient URL path sanitization. Attackers can traverse out of their

9.1 **CVE-2026-7302** Lmsys sglang
SGLangs multimodal generation runtime is vulnerable to an unauthenticated path traversal vulnerability, allowing an attacker to write arbitrary files anywhere the server process has write access, by including ../ sequences in the upload filename when sent to s

9.1 **CVE-2026-41947** Dify dify
Dify before version 1.14.2 contains an authorization bypass vulnerability that allows authenticated editor users to set and enable trace configurations for any application regardless of tenant ownership. Attackers can exploit missing tenant ownership checks in

9.1 **CVE-2023-24215**
Incorrect access control in the /uci/get/ endpoint of NOVUS AirGate 4G firmware v1.1.16 allows unauthenticated attackers to obtain administrator credentials via a crafted POST request.

Ransomware

No leak-site posts collected.

New data breaches 1

Addi addi.com FINANCE 34,532,941 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.