Daily brief, Wednesday, May 13, 2026

May 12, 8:00 PM to May 13, 8:00 PM ET

Generated Nov 7, 2026, 1:46 AM ET

0	0	0	32	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

32 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

32

9.1 **CVE-2026-41225** F5 big-ip access policy manager

iControl REST API. An attacker gains arbitrary command execution. Patch the iControl REST API to a supported version.

9.8 **CVE-2026-0263** Palo Alto Networks pan-os

A buffer overflow vulnerability in the IKEv2 processing of Palo Alto Networks PAN-OS® software allows an unauthenticated network-based attacker to execute arbitrary code with elevated privileges on the firewall, or cause a denial of service (DoS) condition. Pa

9.8 **CVE-2026-0264** Palo Alto Networks pan-os

A buffer overflow vulnerability in the DNS proxy and DNS Server features of Palo Alto Networks PAN-OS® Software allows an unauthenticated attacker with network access to cause a denial of service (DoS) condition (all PAN-OS platforms except Cloud NGFW and Pris

9.1 **CVE-2026-0258** Palo Alto Networks pan-os

A server-side request forgery (SSRF) vulnerability in the IKEv2 implementation of Palo Alto Networks PAN-OS® software allows an unauthenticated attacker to cause the firewall to send network requests to unintended destinations or cause a denial of service (DoS

9.8 **CVE-2026-42062** ELECOM WRC-BE72XSD-B

ELECOM wireless LAN access point devices contain an OS command injection in processing of username parameter. If processing a crafted request, an arbitrary OS command may be executed. No authentication is required.

9.8 **CVE-2026-40621** ELECOM WRC-BE72XSD-B

ELECOM wireless LAN access point devices do not require authentication to access some specific URLs. The affected product may be operated without authentication.

9.8 **CVE-2026-32661** Canon Marketing Japan GUARDIANWALL MailSuite (On-premises version)

Stack-based buffer overflow vulnerability exists in GUARDIANWALL MailSuite and GUARDIANWALL Mail Security Cloud (SaaS version). If a remote attacker sends a specially crafted request to the product's web service, arbitrary code may be executed when the product

9.9 **CVE-2026-41050** Suse rancher fleet

Fleet's Helm deployer did not fully apply ServiceAccount impersonation in two code paths, allowing a tenant with git push access to a Fleet-monitored repository to read secrets from any namespace on every downstream cluster targeted by their `GitRepo`.

10.0 **CVE-2026-43997** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, it is possible to obtain the host Object. There are various ways to use the host Object, to escape the sandbox, one example would be using HostObject.getOwnPropertySymbols to obtain Symbol(nodejs.u

10.0 **CVE-2026-44005** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. From 3.9.6 to 3.10.5, vm2's bridge exposes mutable proxies for real host-realm intrinsic prototypes and then forwards sandbox writes into the underlying host objects with otherReflectSet() and otherReflectDefinePro

10.0 **CVE-2026-44006** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, It is possible to reach BaseHandler.getPrototypeOf, which can be used to get arbitrary prototypes. This vulnerability is fixed in 3.11.0.

9.9 **CVE-2026-43999** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.0, NodeVM's builtin allowlist can be bypassed when the module builtin is allowed (including via the '*' wildcard). The module builtin exposes Node's Module._load(), which loads any module by name dire

9.9 **CVE-2026-44442** Frappe erpnext

ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 16.9.1, certain endpoints failed to enforce proper authorization checks, allowing users to modify data beyond their permitted role. This vulnerability is fixed in 16.9.1.

9.8 **CVE-2020-37168**

Ecommerce Systempay 1.0 contains a weak cryptographic implementation vulnerability that allows attackers to brute force the 16-character production secret key used for payment signature generation. Attackers can extract payment form data and signatures from PO

9.8 **CVE-2026-44008** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.2, the new method neutralizeArraySpeciesBatch works with objects from the other side but can call into this side via getter on the array prototype exposing objects of the wrong side into the sandbox.

9.8 **CVE-2026-44009** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.2, VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This vulnerability is

9.8 **CVE-2026-45411** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.3, it is possible to catch a host exception using the yield* expression inside an async generator. When the generator is closed using the return function, the value is awaited on and exceptions thrown

9.8 **CVE-2026-42031** Okfn ckan DETECTION

+1 more CVEs in the same release

CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.10 and 2.11.5, a vulnerability in datastore_search_sql allowed attackers to inject SQL in order to gain access to private resources and PostgreSQL system

9.8 **CVE-2026-8500**

Web::Passwd versions through 0.03 for Perl is vulnerable to RCE. Web::Passwd is a small CGI application for managing htpasswd files using the htpasswd command. The user parameter is not validated or escaped, and is used as the last argument on the command line

9.6 **CVE-2026-42557** Jupyter jupyterlab

jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. Prior to 4.5.7, JupyterLab's HTML sanitizer allowlists data-commandlinker-command and data-commandlinker-args on button elements, wh

11 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Canada Life canadalife.com 237,810 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.