Daily brief, Tuesday, May 19, 2026

May 18, 8:00 PM to May 19, 8:00 PM ET

Generated Nov 7, 2026, 12:34 AM ET

0	0	0	31	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

31 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

31

9.8 **CVE-2026-47323** Apache camel EXPLOIT CODE

Camel-CXF and Camel-Knative Message Header Injection via Missing Inbound Filtering The CXF and Knative HeaderFilterStrategy implementations (CxfRsHeaderFilterStrategy in camel-cxf-rest, CxfHeaderFilterStrategy in camel-cxf-transport, and KnativeHttpHeaderFilte

9.8 **CVE-2026-43493** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: crypto: pcrypt - Fix handling of MAY_BACKLOG requests MAY_BACKLOG requests can return EBUSY. Handle them by checking for that value and filtering out EINPROGRESS notifications.

9.8 **CVE-2026-8956** Mozilla firefox

Integer overflow in the Networking: JAR component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.

9.6 **CVE-2026-8953** Mozilla firefox

Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.

9.6 **CVE-2026-8959** Mozilla firefox

Sandbox escape due to incorrect boundary conditions in the Widget: Win32 component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.

9.3 **CVE-2026-8950** Mozilla firefox

Same-origin policy bypass in the Networking: HTTP component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.

9.1 **CVE-2026-8948** Mozilla firefox

Same-origin policy bypass in the DOM: Networking component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.

10.0 **CVE-2026-43633**

HestiaCP versions 1.9.0 through 1.9.4 contain a deserialization vulnerability in the web terminal component caused by a session format mismatch between PHP and Node.js that allows unauthenticated remote attackers to achieve root-level code execution. Attackers

10.0 **CVE-2026-34234** DETECTION

CtrlPanel is open-source billing software for hosting providers. In versions 1.1.1 and prior, the web-based installer (public/installer/index.php) is vulnerable to unauthenticated Remote Code Execution (RCE) because it performs the install.lock check only afte

9.9 **CVE-2026-33642** Kovidgoyal kitty

Kitty is a cross-platform GPU based terminal. In versions 0.46.2 and below, the handle_compose_command() function in kitty/graphics.c performs bounds validation on composition offsets using unsigned 32-bit arithmetic that is subject to integer wrapping, potent

9.8 **CVE-2026-4885**

The Piotnet Addons for Elementor Pro plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the 'pafe_ajax_form_builder' function in all versions up to, and including, 7.1.70. The plugin uses an incomplete extension

9.8 **CVE-2026-45434** Apache ofbiz DETECTION

Improper Authentication vulnerability in Apache OFBiz via Password-Change Logic Flaw Leading to Remote Code Execution This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.

9.8 **CVE-2026-4883** DETECTION

The Piotnet Forms plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the 'piotnetforms_ajax_form_builder' function in all versions up to, and including, 2.1.40. The plugin uses an incomplete extension blacklist t

9.8 **CVE-2026-44159**

Tyler Identity Local (TID-L) uses documented, default administrative credentials. Users are not required to change the credentials before deployment. TID-L has not been distributed since December 2020, and has not been supported since 2021.

9.8 **CVE-2026-30117**

scalar/astro v0.1.13 was discovered to contain an arbitrary file upload vulnerability in the the scalar_url query parameter of the Scalar Proxy endpoint. This vulnerability allows attackers to execute arbitrary code via uploading a crafted SVG file.

9.8 **CVE-2026-30118**

scalar/astro v0.1.13 was discovered to contain a Server-Side Request Forgery (SSRF) in the scalar_url query parameter of the Scalar Proxy endpoint. This vulnerability allows unauthenticated attackers to force the backend server to send HTTP requests to attacke

9.8 **CVE-2026-31070**

The LalanaChami Pharmacy Management System (commit 5c3d028) allows unauthenticated remote attackers to escalate privileges by self-assigning an administrative role during registration. The /api/user/signup endpoint fails to validate the role parameter in the r

9.8 **CVE-2026-31072**

The JSONSerializer and CBORSerializer in APScheduler (all versions including 3.10.x and 4.0.0a5) are vulnerable to Remote Code Execution (RCE) via Insecure Deserialization. The unmarshal_object function allows for arbitrary class instantiation and state inject

9.8 **CVE-2026-37281**

An OS command injection vulnerability in the /stream-to-vlc Express route in hitarth-gg Zenshin before 2.7.0 allows remote attackers to execute arbitrary commands via the url parameter.

9.8 **CVE-2026-36829**

An authentication bypass vulnerability exists in the embedded HTTP server of Panabit PAP-XM320 up to and including v7.7. The server validates session cookies using a filesystem existence check based on a user-controlled cookie value without proper sanitization

11 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

CTT ctt.pt 468,124 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.