Daily brief, Monday, February 23, 2026

Feb 22, 7:00 PM to Feb 23, 7:00 PM ET

Generated Nov 7, 2026, 4:10 PM ET

0	0	0	9	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

9 new critical CVEs.

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

9

9.8 **CVE-2026-3062** Google chrome

Out of bounds read and write in Tint in Google Chrome on Mac prior to 145.0.7632.116 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)

9.1 **CVE-2026-3061** Google chrome

Out of bounds read in Media in Google Chrome prior to 145.0.7632.116 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)

10.0 **CVE-2026-23693** DETECTION

ElementsKit Elementor Addons – Advanced Widgets & Templates Addons for Elementor (elementskit-lite) WordPress plugin versions prior to 3.7.9 expose the REST endpoint /wp-json/elementskit/v1/widget/mailchimp/subscribe without authentication. The endpoint accept

9.8 **CVE-2025-70327** Totolink x5000r firmware

TOTOLINK X5000R v9.1.0cu_2415_B20250515 contains an argument injection vulnerability in the setDiagnosisCfg handler of the /usr/sbin/lighttpd executable. The ip parameter is retrieved via websGetVar and passed to a ping command through CsteSystem without valid

9.1 **CVE-2026-23552** Apache camel

Cross-Realm Token Acceptance Bypass in KeycloakSecurityPolicy Apache Camel Keycloak component. The Camel-Keycloak KeycloakSecurityPolicy does not validate the iss (issuer) claim of JWT tokens against the configured realm. A token issued by one Keycloak realm i

9.8 **CVE-2026-24494**

SQL Injection vulnerability in the /api/integrations/getintegrations endpoint of Order Up Online Ordering System 1.0 allows an unauthenticated attacker to access sensitive backend database data via a crafted store_id parameter in a POST request.

9.1 **CVE-2026-2588** Timlegge crypt\

Crypt::NaCl::Sodium versions through 2.001 for Perl has an integer overflow flaw on 32-bit systems. Sodium.xs casts a STRLEN (size_t) to unsigned long long when passing a length pointer to libsodium functions. On 32-bit systems size_t is typically 32-bits whil

9.3 **CVE-2025-41002**

SQL injection vulnerability in Infoticketing. This vulnerability allows an unauthenticated attacker to retrieve, create, update, and delete the database by sending a POST request using the 'code' parameter in '/components/cart/cartApplyDiscount.php'.

9.1 **CVE-2025-70043**

An issue pertaining to CWE-295: Improper Certificate Validation was discovered in Ayms node-To master. The application disables TLS/SSL certificate validation by setting 'rejectUnauthorized': false in TLS socket options

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. 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.