Daily brief, Saturday, June 20, 2026

Jun 19, 8:00 PM to Jun 20, 8:00 PM ET

Generated Nov 4, 2026, 5:02 PM ET

0	0	0	7	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 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

7

9.9 **CVE-2026-5366** Prefect prefect

Prefect version 3.6.23 is vulnerable to remote code execution due to improper handling of user-controlled input in the `GitRepository` storage class. The `commit_sha` parameter, which is passed to git commands, lacks validation and does not include a `--` sepa

9.8 **CVE-2026-11551**

The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.29. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possibl

9.8 **CVE-2019-25763**

WordPress Ultimate Addons for Beaver Builder 1.2.4.1 contains an authentication bypass vulnerability that allows attackers to gain unauthorized access by exploiting the social media login form functionality. Attackers can submit a POST request to the admin-aja

9.8 **CVE-2022-50972**

WooCommerce 7.1.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary PHP code by injecting shell commands through the product-type parameter. Attackers can send requests to the class-wc-meta-box-product-images.php endpoin

9.8 **CVE-2024-58351**

Flowise before 2.1.4 allows configuration to be injected into the Chainflow during execution via the overrideConfig option, supported in both the frontend web integration and the backend Prediction API. Because this feature is enabled by default with no allow-

9.5 **CVE-2026-48909** DETECTION

SP LMS (com_splms) < 4.1.4 by JoomShaper deserializes user-controlled cookie data without validation, enabling an unauthenticated remote attacker to execute arbitrary code on the server.

9.1 **CVE-2026-9265**

Crypt::OpenSSL::PKCS12 versions before 1.96 for Perl permits a heap OOB read in print_attribute UTF8STRING path. print_attribute() copies a UTF8STRING ASN.1 attribute value into a heap buffer sized exactly to its declared length via strncpy, leaving no NUL ter

Ransomware

No leak-site posts collected.

New data breaches 1

JCPenney jcpenny.com 368,418 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. CVE IDs link to the full record on Watch Floor.