Daily brief, Wednesday, June 10, 2026

Jun 9, 8:00 PM to Jun 10, 8:00 PM ET

Generated Nov 5, 2026, 2:31 AM ET

0	0	0	25	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

25 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

25

9.1 **CVE-2026-0274** Palo Alto Networks cortex xsiam commvaultsecurityiq marketplace

An improper validation of credentials vulnerability in the CommvaultSecurityIQ integration for Cortex XSOAR and Cortex XSIAM allows an unauthenticated attacker to access and modify protected resources.

10.0 **CVE-2026-46695**

+1 more CVEs in the same release

Boxlite is a sandbox service that allows users to create lightweight virtual machines (Boxes) and launch OCI containers within them to run untrusted code. Prior to version 0.9.0, Boxlite does not restrict the kernel capabilities available inside the container,

9.9 **CVE-2026-45552**

+1 more CVEs in the same release

Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, the install blueprint declares only bp.before_request ? @jwt_required() (app/routes/install/routes.py:36-39). The individual endpoints install

9.9 **CVE-2026-45556**

Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, POST /waf/<service>/<server_ip>/rule/<rule_id>/save accepts a config_file_name form field that is passed straight through to config_mod.master

9.9 **CVE-2026-50545**

+4 more CVEs in the same release

Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, the Environment.spec.runtime.podSpec / spec.builder.podSpec passthrough lacked validation, an

9.8 **CVE-2025-66276** Qnap qts

QuTS hero is not affected. We have already fixed the vulnerability in the following version: QTS 5.2.7.3256 build 20250913 and later

9.8 **CVE-2025-6254**

The Doctreat Core plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.6.8. This is due to the doctreat_process_registration() function not properly restricting the roles that a user can register with. This makes i

9.6 **CVE-2026-53470** Kebev2v migration assessment

A flaw was found in migration-planner. An authenticated attacker could exploit an improper access control vulnerability in the `/api/v1/sources/{id}/image-url` endpoint. This flaw allows the attacker to bypass an ownership check and obtain presigned S3 URLs fo

9.6 **CVE-2026-53471** Kebev2v migration assessment

A flaw was found in migration-planner. The agent-API middleware processes JSON Web Tokens (JWTs) for authentication, but its UpdateSourceInventory and UpdateAgentStatus handlers fail to validate the source_id claim within these tokens against the requested sou

9.6 **CVE-2026-53474** Kebev2v migration assessment

A flaw was found in migration-planner. A remote authenticated attacker could exploit this vulnerability by uploading a specially crafted RVTools .xlsx file. Due to improper input sanitization, malicious SQL embedded within a spreadsheet cell is executed when c

9.6 **CVE-2026-53476** Kubev2v assisted migration agent

A flaw was found in assisted-migration-agent. An unauthenticated attacker, located on the same local area network (LAN), can exploit a path traversal vulnerability. By crafting a specially designed gzipped tarball, the attacker can bypass security checks and w

9.3 **CVE-2026-45328** Espressif esp-idf

ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.4 and 6.0, the esp_tee component exposes secure-service wrappers in esp_secure_services.c and esp_secure_services_iram.c that bridge calls from the user application (i.e.

9.3 **CVE-2026-53475** Kubev2v assisted migration agent

A flaw was found in assisted-migration-agent. The application hardcodes insecure Transport Layer Security (TLS) connections when communicating with vCenter. This vulnerability allows a Man-in-the-Middle (MITM) attacker to intercept and harvest vCenter administ

9.1 **CVE-2026-26240** Qnap file station

+1 more CVEs in the same release

A buffer overflow vulnerability has been reported to affect File Station 5. The remote attackers can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5243

9.1 **CVE-2026-9067**

The Schema & Structured Data for WP & AMP WordPress plugin before 1.60 does not check user capabilities on its frontend AJAX file-upload handlers and does not validate the actual content of uploaded files against the endpoint's intended media type, allowing un

9.1 **CVE-2026-45550**

Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, PUT /smon/check (app/routes/smon/routes.py:117-138) gates only on roxywi_common.check_user_group_for_flask() — which validates that the caller

9.1 **CVE-2026-53469** Kebev2v migration assessment

A flaw was found in migration-planner. An authenticated user can exploit this vulnerability by sending a DELETE request to the /api/v1/sources route, which lacks proper authorization and filtering. This allows for the destruction of all customer data, includin

9.1 **CVE-2026-50638** Pevans metrics\

Metrics::Any::Adapter::DogStatsd versions before 0.04 for Perl does not protect against metric injections. The statsd protocol (and extensions such as dogstatsd) allow mutiple metrics, separated by newlines, to be sent per packet. Metrics::Any::Adapter::DogSta

Ransomware

No leak-site posts collected.

New data breaches 1

University of Nottingham nottingham.ac.uk 454,635 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.