Daily brief, Wednesday, July 29, 2026

Jul 28, 8:00 PM to Jul 29, 8:00 PM ET

Generated Nov 3, 2026, 4:37 AM ET

0	1	0	43	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 43 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

5.3 **CVE-2026-20316** Cisco Secure Firewall Management Center (FMC) CISA KEV

An unauthenticated attacker gains ability to log in to Cisco Secure Firewall Management Center using a low-privileged account.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

43

10.0 **CVE-2026-33267** Apache traffic server

Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.14, from 10.1.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.

10.0 **CVE-2026-57834** Apache traffic server

Apache Traffic Server allows request smuggling if chunked messages are malformed. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or

10.0 **CVE-2026-58150** Apache traffic server

Apache Traffic Server does not reject Transfer-Encoding in HTTP/2 requests, allowing downgrade request smuggling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended

10.0 **CVE-2026-58162** Apache traffic server

The Apache Traffic Server certifier plugin generates certificates based on attacker-controlled client SNI. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgr

10.0 **CVE-2026-54735** Prebid prebid server

Prebid Server is an open-source solution for running real-time advertising auctions in the cloud. Prior to version 4.4.0, certain bidder adapters in Prebid Server interpolate user-supplied parameters into outbound request URLs without properly validating host

10.0 **CVE-2026-16326**

In consul-mcp-server, versions 0.1.0 up to 0.1.3 did not properly isolate session state in stateless mode, which may allow one client's Consul authentication token to be used for subsequent requests from other clients. This vulnerability (CVE-2026-16326) is fi

10.0 **CVE-2026-67429**

Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, image.download and related file-writing modules use caller-controlled output_dir instead of validate_path_with_env_config and its FLYTO_SANDBOX_DIR confinement, allowing

9.9 **CVE-2026-63227**

An unrestricted SCORM file upload vulnerability in Koollab LMS allowed an authenticated module designer to upload a SCORM package containing a PHP webshell to a publicly accessible directory and execute arbitrary code on the server.

9.9 **CVE-2026-63232**

+2 more CVEs in the same release

A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the assessment reinforcement endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and exe

9.9 **CVE-2026-54680**

Logging operator automates the deployment and configuration of Kubernetes logging pipelines. Prior to 6.6.0, the Fluentd configuration renderer FluentRender in pkg/sdk/logging/model/render/fluent.go writes CRD strings such as Flow record_transformer.records va

9.8 **CVE-2026-18072** DETECTION

The Advanced Responsive Video Embedder for Rumble, Odysee, YouTube, Vimeo, Kick … plugin for WordPress is vulnerable to Authentication Bypass via a Hardcoded Backdoor in version 10.8.7. The vulnerability exists because the `_arve_uc_init()` function — register

9.8 **CVE-2026-13423**

The Streamit WordPress theme through 4.5.0 does not perform any authorization or nonce verification on one of its unauthenticated AJAX routes, which invokes an attacker-supplied PHP function with an attacker-supplied argument array, allowing unauthenticated at

9.8 **CVE-2026-18191**

VIN-DS783E-E6 developed by Vacron has a Hidden Functionality vulnerability, allowing unauthenticated remote attackers to exploit a specific hidden function to obtain the administrator credentials of the device.

9.8 **CVE-2025-10656**
The Spreadsheet Price Changer for WooCommerce and WP E-commerce – Light plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.4.37 vi the user_filter function. This makes it possible for unauthenticated attackers t

9.8 **CVE-2026-59243** Apache apache-airflow-providers-fab
The FAB auth manager's Azure AD OAuth login defaulted `verify_signature=False` when decoding the ID token, so an attacker able to present a forged or unsigned (`alg:none`) ID token to the OAuth callback could bypass authentication and log in as an arbitrary us

9.8 **CVE-2026-14900**
The Cost Calculator Builder PRO plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.0.3 via the js_to_php function. This is due to insufficient sanitization of the orderDetails[*].originalValue field, which is in

9.8 **CVE-2026-65883** Aimy-Extensions aimy captcha-less form guard
Joomla Extension - aimy-extensions.com - RCE via PHP object injection in Aimy Captcha-Less Form Guard 18.0 - 20.0 - A forged clfgd field allows PHP objection injection and thereby remote code execution.

9.8 **CVE-2026-65884** Balbooa gridbox
Joomla Extension - balbooa.com - Privilege Escalation in Gridbox < 2.20.2 - The registration method allows users provided usergroup IDs, allowing unauthenticated actors to register new accounts with administrative permissions.

9.8 **CVE-2026-65890** Balbooa gridbox
Joomla Extension - balbooa.com - Unauthenticated SQL injection in Gridbox < 2.20.2 - Multiple SQLi vectors allow unauthenticated actors to inject SQL in queries.

9.8 **CVE-2026-65887** Balbooa gridbox
Joomla Extension - balbooa.com - Unauthenticated arbitrary password reset in Gridbox < 2.20.2 - The resetPassword method allows actors to reset any user password, allowing to login and act as these users - excluding super admins.

21 more critical CVEs in this window: see the dashboard

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. CVE IDs link to the full record on Watch Floor.