Daily brief, Saturday, August 1, 2026

Jul 31, 8:00 PM to Aug 1, 8:00 PM ET

Generated Nov 3, 2026, 1:48 AM ET

0	0	0	10	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

10 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

10

9.9 **CVE-2026-67330**

@better-auth/scim (a better-auth plugin) versions >= 1.4.0-beta.27 through <= 1.6.21 and >= 1.7.0-beta.0 through <= 1.7.0-beta.9 contain an authorization bypass. SCIM token issuance did not reject provider IDs already used by existing SSO, SAML, OIDC, generic

9.8 **CVE-2026-15964**

The Single Sign On For TNG plugin for WordPress is vulnerable to Authentication Bypass via unauthenticated password reset in all versions up to, and including, 2.0.0. This is due to the `ssoprocess_ajax()` function — registered on `wp_ajax_nopriv_ssoprocess_aj

9.8 **CVE-2026-66402** Freerdp freerdp

FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains multiple TLS certificate identity validation weaknesses in tls_verify_certificate(), tls_match_hostname(), and x509_utils_get_dns_names(). Because FreeRDP performs custom Common Name and DNS SAN stri

9.8 **CVE-2026-67289** Freerdp freerdp

FreeRDP before 3.29.0 (affected versions <= 3.28.0) does not validate CRLF and control characters in the server-controlled RDP redirection TargetNetAddress field. This value is copied into the client's ServerHostname and, when the client connects through an HT

9.8 **CVE-2026-67324** Gitpython Project gitpython

GitPython 3.1.50 fails to recognize joined short-option forms such as -u<value> (the short form of --upload-pack=<value>) when enforcing its default unsafe-option gate. When an application passes attacker-influenced clone options into Repo.clone_from(..., mult

9.8 **CVE-2026-67341**

ArcadeDB versions before 26.7.2 fail to enforce scripting authorization checks on the SQL DEFINE FUNCTION statement with LANGUAGE js. Attackers with database access can execute arbitrary JavaScript code by submitting DEFINE FUNCTION statements, bypassing secur

9.8 **CVE-2026-67342**

ArcadeDB versions before 26.7.2 contain an authorization bypass vulnerability in HTTP handlers for time series, batch, Prometheus, and Grafana endpoints that fail to validate database access permissions. Attackers can access and modify databases they are not a

9.3 **CVE-2026-67308**

Wazuh workflows before 44bf114 contain a shell injection vulnerability in GitHub Actions that allows attackers to execute arbitrary commands by submitting pull requests with crafted VERSION.json files. Attackers can inject shell metacharacters into environment

9.1 **CVE-2026-3141**

The FormGent plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the /wp-json/formgent/responses/attachments REST API endpoint in all versions up to, and including, 1.9.2 This is due to the REST API r

9.1 **CVE-2026-13596**

The Participants Database WordPress plugin before 2.7.8.4 does not properly sanitize and escape a user-supplied parameter before using it in a SQL query, allowing unauthenticated attackers to perform SQL injection attacks.

Ransomware

No leak-site posts collected.

New data breaches 1

SplitVPN splitvpn.io 865,336 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.