Daily brief, Monday, August 17, 2026

Aug 16, 8:00 PM to Aug 17, 8:00 PM ET

Generated Nov 2, 2026, 10:16 AM ET

0	1	0	62	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 62 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.4 **CVE-2025-62593** Ray-Project Ray CISA KEV DETECTION

Ray-Project Ray contains a code injection vulnerability that could allow remote code execution. Developers using Ray as a development tool may be exposed to this vulnerability exploitable through Firefox and Safari.

New public exploit code

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

New critical CVEs

62

9.4 **CVE-2025-62593** Ray-Project Ray KEV EXPLOIT CODE DETECTION

Ray-Project Ray contains a code injection vulnerability that could allow remote code execution. Developers using Ray as a development tool may be exposed to this vulnerability exploitable through Firefox and Safari.

9.4 **CVE-2026-19478** GitLab GitLab EXPLOIT CODE DETECTION

All versions of GitLab CE/EE from 18.2 before 18.11.11, 19.0 before 19.0.8, 19.1 before 19.1.6, and 19.2 before 19.2.4 are affected. An attacker gains the ability to remotely modify or delete public projects and user data. Upgrade to the latest version of GitL

9.8 **CVE-2026-74872** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain an arbitrary code execution vulnerability in the Whirlpool hash implementation that uses broad glob patterns to load .so modules without integrity verification. Attackers can place malicious .so files matching the

9.8 **CVE-2026-74875** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 silently skip JSON schema validation when the jsonschema library is not installed, allowing malformed metadata to be accepted. Attackers can remove the jsonschema package or supply unknown metadata format versions to bypas

9.8 **CVE-2026-74876** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain a vulnerability in PublicKeyBundle.from_dict() that creates key bundles from untrusted data without verifying signatures. Attackers can call from_dict() followed by to_identity() without signature verification to e

9.8 **CVE-2026-74878** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 use an in-memory rate limiter for TOTP brute-force protection that is not shared across workers and is lost on server restart. Attackers can distribute authentication attempts across multiple server instances or retry imme

9.8 **CVE-2026-74880** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 accept refresh tokens as URL query parameters in keyserver and telemetry server routes. Attackers can extract tokens from server logs, proxy logs, browser history, and HTTP Referer headers to gain unauthorized access.

9.8 **CVE-2026-74886** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain a plugin sandbox bypass vulnerability where the PluginImportGuard blocks a different set of modules than the AST analyzer's DANGEROUS_MODULES set. Attackers can bypass AST analysis through string obfuscation or enc

9.8 **CVE-2026-74889** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 use HKDF with no salt and static info parameter in key normalization functions, reducing entropy extraction and determinism. Attackers can exploit predictable key derivation with identical inputs to weaken cryptographic se

9.8 **CVE-2026-74891** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain hardcoded database credentials in standalone server configuration files. Attackers on the same network can access PostgreSQL databases using well-known default credentials to retrieve sensitive data.

9.8 **CVE-2026-74894** Jahlives openssl encrypt

openssl_encrypt before 1.4.0 contains an authentication bypass vulnerability in the verify_api_token function that accepts any non-empty Bearer token string without validation. Attackers can upload arbitrary public keys, enumerate all keys, and revoke keys bel

9.8 **CVE-2026-74895** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 fail to apply sandbox restrictions in the default process isolation mode for plugin execution. Attackers can execute malicious plugins with unrestricted access to the filesystem, network, subprocess execution, and all Pyth

9.8 **CVE-2026-74896** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain a sandbox escape vulnerability in the DangerousPatternVisitor AST analyzer that fails to detect dunder attribute traversal techniques. Attackers can use __class__, __bases__, __subclasses__(), and __globals__ chain

9.8 **CVE-2026-74899** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain a sandbox escape vulnerability in IsolatedPluginExecutor that exposes Python type objects in restricted exec() builtins. Attackers can traverse the Python class hierarchy via __class__.__mro__.__subclasses__() to a

9.8 **CVE-2026-74900** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain a critical vulnerability in pqc.py where KEM decapsulation failures silently fall back to simulation mode, generating a deterministic shared secret from only 16 bytes of the private key and publicly available encap

9.8 **CVE-2026-74901** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.0 contain an authentication bypass vulnerability in pqc.py where AES-GCM decryption failures trigger fallback to unauthenticated AES-CTR mode. Attackers can modify ciphertext in transit to bypass integrity verification and p

9.8 **CVE-2026-50772**

An issue in Squirro Cognitive Search < 3.14.2 allows a remote attacker to execute arbitrary code via a crafted payload to the password reset function.

9.1 **CVE-2026-51346**

SQL Injection vulnerability in StudIP 6.0.x before 6.0.3 and 5.4.x before 5.4.12 allows a remote attacker to execute arbitrary code and obtain sensitive information via the store() functions.

9.8 **CVE-2026-50770**

An issue in Squirro Cognitive Search before v.3.14.2 allows a remote attacker to escalate privileges via a crafted request.

9.8 **CVE-2026-50774**

An issue in GAPTEQ Designer v.3.5 allows a remote attacker to escalate privileges via the Company Manger role.

42 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.