Daily brief, Thursday, March 26, 2026

Mar 25, 8:00 PM to Mar 26, 8:00 PM ET

Generated Nov 7, 2026, 10:47 AM ET

0	1	0	17	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 17 new critical CVEs, 2 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.4 **CVE-2026-33634** Aquasecurity Trivy CISA KEV

Embedded malicious code in Aquasecurity Trivy gives an attacker access to CI/CD secrets, including tokens, SSH keys, cloud credentials, and database passwords.

New public exploit code

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

New critical CVEs

17

9.4 **CVE-2026-33634** Aquasecurity Trivy KEV EXPLOIT CODE

Embedded malicious code in Aquasecurity Trivy gives an attacker access to CI/CD secrets, including tokens, SSH keys, cloud credentials, and database passwords.

9.9 **CVE-2026-33897** Linuxcontainers incus

Incus is a system container and virtual machine manager. Prior to version 6.23.0, instance template files can be used to cause arbitrary read or writes as root on the host server. Incus allows for pongo2 templates within instances which can be used at various

9.1 **CVE-2026-27815** Linuxfoundation everest

EVerest is an EV charging software stack. Prior to versions to 2026.02.0, ISO15118_chargerImpl::handle_session_setup copies a variable-length payment_options list into a fixed-size array of length 2 without bounds checking. With schema validation disabled by d

9.1 **CVE-2026-27816** Linuxfoundation everest

EVerest is an EV charging software stack. Prior to versions to 2026.02.0, ISO15118_chargerImpl::handle_update_energy_transfer_modes copies a variable-length list into a fixed-size array of length 6 without bounds checking. With schema validation disabled by de

9.8 **CVE-2026-26213** Thingino thingino firmware

thingino-firmware versions up to the firmware-2026-03-16 release contains an unauthenticated os command injection vulnerability in the WiFi captive portal CGI script that allows remote attackers to execute arbitrary commands as root by injecting malicious code

9.8 **CVE-2026-4809**

plank/laravel-mediable through version 6.4.0 can allow upload of a dangerous file type when an application using the package accepts or prefers a client-supplied MIME type during file upload handling. In that configuration, a remote attacker can submit a file

9.9 **CVE-2026-33396** Hackerbay oneuptime

OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.35, a low-privileged authenticated user (ProjectMember) can achieve remote command execution on the Probe container/host by abusing Synthetic Monitor Playwright script exe

9.8 **CVE-2014-125112** Miyagawa plack\

Plack::Middleware::Session::Cookie versions through 0.21 for Perl allows remote code execution. Plack::Middleware::Session::Cookie versions through 0.21 has a security vulnerability where it allows an attacker to execute arbitrary code on the server during des

9.8 **CVE-2026-33670** B3log siyuan

SiYuan is a personal knowledge management system. Prior to version 3.6.2, the /api/file/readDir interface was used to traverse and retrieve the file names of all documents under a notebook. Version 3.6.2 patches the issue.

9.8 **CVE-2026-30457** Thedaylightstudio dwoo

An issue in the /parser/dwoo component of Daylight Studio FuelCMS v1.5.2 allows attackers to execute arbitrary code via crafted PHP code.

9.8 **CVE-2026-33942** Saloon saloon

Saloon is a PHP library that gives users tools to build API integrations and SDKs. Versions prior to 4.0.0 used PHP's unserialize() in AccessTokenAuthenticator::unserialize() to restore OAuth token state from cache or storage, with allowed_classes => true. An

9.1 **CVE-2026-33183** Saloon saloon

Saloon is a PHP library that gives users tools to build API integrations and SDKs. Prior to version 4.0.0, fixture names were used to build file paths under the configured fixture directory without validation. A name containing path segments (e.g. ../traversal

9.8 **CVE-2026-33669** B3log siyuan

SiYuan is a personal knowledge management system. Prior to version 3.6.2, document IDs were retrieved via the /api/file/readDir interface, and then the /api/block/getChildBlocks interface was used to view the content of all documents. Version 3.6.2 patches the

10.0 **CVE-2026-33494** Ory oathkeeper

ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. Versions prior to 26.2.0 are vulnerable to an authorization bypass via HTTP path traversal. An attacker can craft a

9.1 **CVE-2026-33152** Tandoor recipes

Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, Tandoor Recipes configures Django REST Framework with BasicAuthentication as one of the default authentication backends. The AllAut

9.8 **CVE-2026-33640** Getoutline outline

Outline is a service that allows for collaborative documentation. Outline implements an Email OTP login flow for users not associated with an Identity Provider. Starting in version 0.86.0 and prior to version 1.6.0, Outline does not invalidate OTP codes based

9.1 **CVE-2026-30458** Thedaylightstudio fuel cms

An issue in Daylight Studio FuelCMS v1.5.2 allows attackers to exfiltrate users' password reset tokens via a mail splitting attack.

Ransomware

No leak-site posts collected.

New data breaches 2

Sound Radix	soundradix.com	292,993 accounts
Scuf Gaming	scufgaming.com	128,683 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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.