Daily brief, Friday, March 27, 2026

Mar 26, 8:00 PM to Mar 27, 8:00 PM ET

Generated Nov 7, 2026, 10:37 AM ET

0	1	0	36	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 36 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2025-53521** F5 BIG-IP CISA KEV

An attacker gains remote code execution and control of the system in F5 BIG-IP, including Application Services Manager and other BIG-IP products.

New public exploit code

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

New critical CVEs

36

9.8 **CVE-2025-53521** F5 BIG-IP KEV

An attacker gains remote code execution and control of the system in F5 BIG-IP, including Application Services Manager and other BIG-IP products.

9.8 **CVE-2026-22738** Vmware spring ai EXPLOIT CODE

In Spring AI, a SpEL injection vulnerability exists in SimpleVectorStore when a user-supplied value is used as a filter expression key. A malicious actor could exploit this to execute arbitrary code. Only applications that use SimpleVectorStore and pass user-s

9.8 **CVE-2026-33701** Linuxfoundation opentelemetry instrumentation for java

OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.26.1, the RMI instrumentation registered a custom endpoint that deserialized incoming data without applying serializat

9.8 **CVE-2026-33728** Datadog dd-trace-java

dd-trace-java is a Datadog APM client for Java. In versions of dd-trace-java 0.40.0 through prior to 1.60.2, the RMI instrumentation registered a custom endpoint that deserialized incoming data without applying serialization filters. On JDK version 16 and earl

9.9 **CVE-2026-33945** Linuxcontainers incus

Incus is a system container and virtual machine manager. Incus instances have an option to provide credentials to systemd in the guest. For containers, this is handled through a shared directory. Prior to version 6.23.0, an attacker can set a configuration key

10.0 **CVE-2026-30302** Coderider-Kilo coderider

The command auto-approval module in CodeRider-Kilo contains an OS Command Injection vulnerability, rendering its whitelist security mechanism ineffective. The vulnerability stems from the incorrect use of an incompatible command parser (the Unix-based shell-qu

9.1 **CVE-2026-27876** Grafana grafana

A chained attack via SQL Expressions and a Grafana Enterprise plugin can lead to a remote arbitrary code execution impact (RCE). This is enabled by a feature in Grafana (OSS), so all users are always recommended to update to avoid future attack vectors going t

9.8 **CVE-2026-33937** Handlebarsjs handlebars

Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, `Handlebars.compile()` accepts a pre-parsed AST object in addition to a template string. The `value` field of a `NumberLiteral` AST node is emitted

9.9 **CVE-2026-33873** Langflow langflow

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.9.0, the Agentic Assistant feature in Langflow executes LLM-generated Python code during its validation phase. Although this phase appears intended to validate ge

9.8 **CVE-2026-30303** Matterai axon code

The command auto-approval module in Axon Code contains an OS Command Injection vulnerability, rendering its whitelist security mechanism ineffective. The vulnerability stems from the incorrect use of an incompatible command parser (the Unix-based shell-quote l

9.8 **CVE-2026-34387** Fleetdm fleet

Fleet is open source device management software. Prior to 4.81.1, a command injection vulnerability in Fleet's software installer pipeline allows an attacker to achieve arbitrary code execution as root (macOS/Linux) or SYSTEM (Windows) on managed hosts when an

9.8 **CVE-2026-33765** Pi-Hole web interface

Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. Versions prior to 6.0 have a critical OS Command Injection vulnerability in the savesettings.php file. The application takes the user

9.8 **CVE-2026-4620** Nec aterm wx3600hp firmware

+1 more CVEs in the same release

OS Command Injection vulnerability in NEC Platforms, Ltd. Aterm Series allows a attacker to execute arbitrary OS commands via network.

9.8 **CVE-2026-27650** Buffalo wcr-1166dhpl firmware

OS Command Injection vulnerability exists in BUFFALO Wi-Fi router products. If this vulnerability is exploited, an arbitrary OS command may be executed on the products.

9.6 **CVE-2026-33976** Streetwriters notesnook desktop

Notesnook is a note-taking app. Prior to version 3.3.11 on Web/Desktop and 3.3.17 on Android/iOS, a stored XSS in the Web Clipper rendering flow can be escalated to remote code execution in the desktop app. The root cause is that the clipper preserves attacker

9.8 **CVE-2026-33993** Locutus locutus

Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Prior to version 3.0.25, the `unserialize()` function in `locutus/php/var/unserialize` assigns deserialized keys to plain objects via bracket notation without filteri

9.8 **CVE-2026-33994** Locutus locutus

Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Starting in version 2.0.39 and prior to version 3.0.25, a prototype pollution vulnerability exists in the `parse_str` function of the npm package locutus. An attacker

9.3 **CVE-2026-1496**

Vulnerable versions of Coverity Connect lack an error handler in the authentication logic for command line tooling that makes it vulnerable to an authentication bypass. A malicious actor with access to the /token API endpoint that either knows or guesses a val

9.8 **CVE-2026-33654** Nanobot nanobot

nanobot is a personal AI assistant. Prior to version 0.1.6, an indirect prompt injection vulnerability exists in the email channel processing module (`nanobot/channels/email.py`), allowing a remote, unauthenticated attacker to execute arbitrary LLM instruction

9.8 **CVE-2026-33890** Franklioxygen mytube

MyTube is a self-hosted downloader and player for several video websites Prior to version 1.8.71, an unauthenticated attacker can register an arbitrary passkey and subsequently authenticate with it to obtain a full admin session. The application exposes passke

15 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

BreachForums Version 5 breachforums.bf 339,778 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.