Daily brief, Tuesday, March 31, 2026

Mar 30, 8:00 PM to Mar 31, 8:00 PM ET

Generated Nov 7, 2026, 9:59 AM ET

0	0	0	37	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

37 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

37

9.8 **CVE-2026-3300** DETECTION

The Everest Forms Pro plugin for WordPress is vulnerable to Remote Code Execution via PHP Code Injection in all versions up to, and including, 1.9.12. This is due to the Calculation Addon's process_filter() function concatenating user-submitted form field valu

9.9 **CVE-2026-34156** Nocobase nocobase DETECTION

NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.28, NocoBase's Workflow Script Node executes user-supplied JavaScript inside a Node.js vm sandbox with a custom require allowl

9.1 **CVE-2026-21861** Basercms basercms

baserCMS is a website development framework. Prior to version 5.2.3, baserCMS contains an OS command injection vulnerability in the core update functionality. An authenticated administrator can execute arbitrary OS commands on the server due to improper handli

9.8 **CVE-2026-34243** Njzjz wenxian

wenxian is a tool to generate BIBTEX files from given identifiers (DOI, PMID, arXiv ID, or paper title). In versions 0.3.1 and prior, a GitHub Actions workflow uses untrusted user input from issue_comment.body directly inside a shell command, allowing potentia

9.8 **CVE-2026-30880** Basercms basercms

baserCMS is a website development framework. Prior to version 5.2.3, baserCMS has an OS command injection vulnerability in the installer. This issue has been patched in version 5.2.3.

9.8 **CVE-2026-32917** Openclaw openclaw

OpenClaw before 2026.3.13 contains a remote command injection vulnerability in the iMessage attachment staging flow that allows attackers to execute arbitrary commands on configured remote hosts. The vulnerability exists because unsanitized remote attachment p

9.8 **CVE-2026-30311** Ridvay auto-approval module

+1 more CVEs in the same release

Ridvay Code's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attem

9.8 **CVE-2026-30312**

DSAI-Cline's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on string-based parsing to validate commands; while it intercepts dangerous

9.1 **CVE-2026-30877** Basercms basercms

baserCMS is a website development framework. Prior to version 5.2.3, there is an OS command injection vulnerability in the update functionality. Due to this issue, an authenticated user with administrator privileges in baserCMS can execute arbitrary OS command

9.8 **CVE-2026-1579** Px4 autopilot

The MAVLink communication protocol does not require cryptographic authentication by default. When MAVLink 2.0 message signing is not enabled, any message -- including SERIAL_CONTROL, which provides interactive shell access -- can be sent by an unauthenticated

9.9 **CVE-2026-33579** Openclaw openclaw

OpenClaw before 2026.3.28 contains a privilege escalation vulnerability in the /pair approve command path that fails to forward caller scopes into the core approval check. A caller with pairing privileges but without admin privileges can approve pending device

9.8 **CVE-2026-30281** Maru neo.maru

An arbitrary file overwrite vulnerability in MaruNuri LLC v2.0.23 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-30276** Deftpdf document translator

An arbitrary file overwrite vulnerability in DeftPDF Document Translator v54.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-30286** Funambol zefiro

An arbitrary file overwrite vulnerability in Funambol, Inc. Zefiro Cloud v32.0.2026011614 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-34041** Nektos act

act is a project which allows for local running of github actions. Prior to version 0.2.86, act unconditionally processes the deprecated ::set-env:: and ::add-path:: workflow commands, which was disabled due to environment injection risks. When a workflow step

9.8 **CVE-2026-30285** Zora zora

An arbitrary file overwrite vulnerability in Zora: Post, Trade, Earn Crypto v2.60.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-30278** Funair fly is fun

An arbitrary file overwrite vulnerability in FLY is FUN Aviation Navigation v35.33 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-30310**

In its design for automatic terminal command execution, Sixth offers two options: Execute safe commands and Execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas if

9.8 **CVE-2026-30283** Peaksel animal sounds and ringtones

An arbitrary file overwrite vulnerability in PEAKSEL D.O.O. NIS Animal Sounds and Ringtones v1.3.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.

9.8 **CVE-2026-34400** Alerta Project alerta

Alerta is a monitoring tool. Prior to version 9.1.0, the Query string search API (q=) was vulnerable to SQL injection via the Postgres query parser, which built WHERE clauses by interpolating user-supplied search terms directly into SQL strings via f-strings.

16 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Cuties AI cuties.ai 144,250 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.