Daily brief, Thursday, April 2, 2026

Apr 1, 8:00 PM to Apr 2, 8:00 PM ET

Generated Nov 7, 2026, 9:37 AM ET

0	1	0	19	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 19 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.8 **CVE-2026-3502** TrueConf Client CISA KEV

An attacker who influences the TrueConf Client update delivery path can substitute a tampered payload, gaining arbitrary code execution when the updater runs it.

New public exploit code

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

New critical CVEs

19

9.8 **CVE-2026-2699** Progress sharefile storage zones controller DETECTION

Customer Managed ShareFile Storage Zones Controller (SZC) allows an unauthenticated attacker to access restricted configuration pages. This leads to changing system configuration and potential remote code execution.

9.1 **CVE-2026-2701** Progress sharefile storage zones controller DETECTION

Authenticated user can upload a malicious file to the server and execute it, which leads to remote code execution.

9.9 **CVE-2026-34838** Intermesh group-office

Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.156, 25.0.90, and 26.0.12, a vulnerability in the AbstractSettingsCollection model leads to insecure deserialization when these settings are loaded. By inj

10.0 **CVE-2026-32871** Jlowin fastmcp

FastMCP is a Pythonic way to build MCP servers and clients. Prior to version 3.2.0, the OpenAPIProvider in FastMCP exposes internal APIs to MCP clients by parsing OpenAPI specifications. The RequestDirector class is responsible for constructing HTTP requests t

9.1 **CVE-2026-34745** Shaneisrael fireshare

Fireshare facilitates self-hosted media and link sharing. Prior to version 1.5.3, the fix for CVE-2026-33645 was applied to the authenticated /api/uploadChunked endpoint but was not applied to the unauthenticated /api/uploadChunked/public endpoint in the same

9.8 **CVE-2026-35053** Hackerbay oneuptime

OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, the Worker service's ManualAPI exposes workflow execution endpoints (GET /workflow/manual/run/:workflowId and POST /workflow/manual/run/:workflowId) without any authen

9.8 **CVE-2024-14034**

Hirschmann HiEOS devices versions prior to 01.1.00 contain an authentication bypass vulnerability in the HTTP(S) management module that allows unauthenticated remote attackers to gain administrative access by sending specially crafted HTTP(S) requests. Attacke

9.8 **CVE-2026-34877** Arm mbed tls

An issue was discovered in Mbed TLS versions from 2.19.0 up to 3.6.5, Mbed TLS 4.0.0. Insufficient protection of serialized SSL context or session structures allows an attacker who can modify the serialized structures to induce memory corruption, leading to ar

9.4 **CVE-2026-33950** Signalk signal k server

Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.24.0-beta.4, there is a privilege escalation vulnerability by Admin Role Injection via /enableSecurity. An unauthenticated attacker can gain full Administrator acc

9.1 **CVE-2026-33615** Mbconnectline mbconnect24

An unauthenticated remote attacker can exploit an unauthenticated SQL Injection vulnerability in the setinfo endpoint due to improper neutralization of special elements in a SQL UPDATE command. This can result in a total loss of integrity and availability.

9.6 **CVE-2026-34931** Hoppscotch hoppscotch

hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, there is an open redirect vulnerability that leads to token exfiltration. With these tokens, the attacker can sign in as the victim to takeover their account. This issue has bee

9.1 **CVE-2026-34758** Hackerbay oneuptime

OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, unauthenticated access to Notification test and Phone Number management endpoints allows SMS/Call/Email/WhatsApp abuse and phone number purchase. This issue has been p

9.8 **CVE-2026-33746** Convoypanel convoy

Convoy is a KVM server management panel for hosting businesses. From version 3.9.0-beta to before version 4.5.1, the JWTService::decode() method did not verify the cryptographic signature of JWT tokens. While the method configured a symmetric HMAC-SHA256 signe

9.9 **CVE-2026-25212** Percona monitoring and management

An issue was discovered in Percona PMM before 3.7. Because an internal database user retains specific superuser privileges, an attacker with pmm-admin rights can abuse the "Add data source" feature to break out of the database context and execute shell command

9.3 **CVE-2026-34932** Hoppscotch hoppscotch

hoppscotch is an open source API development ecosystem. Prior to version 2026.3.0, there is a stored XSS vulnerability that can lead to CSRF. This issue has been patched in version 2026.3.0.

9.8 **CVE-2026-29139** Seppmail secure email gateway

SEPPmail Secure Email Gateway before version 15.0.3 allows account takeover by abusing GINA account initialization to reset a victim account password.

9.9 **CVE-2026-34717** Openproject openproject

OpenProject is an open-source, web-based project management software. Prior to version 17.2.3, the =n operator in modules/reporting/lib/report/operator.rb:177 embeds user input directly into SQL WHERE clauses without parameterization. This issue has been patch

9.1 **CVE-2026-29143** Seppmail secure email gateway

SEPPmail Secure Email Gateway before version 15.0.3 does not properly authenticate the inner message of S/MIME-encrypted MIME entities, allowing an attacker to control trusted headers.

9.1 **CVE-2026-29133** Seppmail secure email gateway

SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to upload PGP keys with UIDs that do not match their email address.

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. 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.