Daily brief, Thursday, May 7, 2026

May 6, 8:00 PM to May 7, 8:00 PM ET

Generated Nov 7, 2026, 2:56 AM ET

0	1	0	29	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 29 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.2 **CVE-2026-6973** Ivanti Endpoint Manager Mobile (EPMM) CISA KEV

An attacker gains remote code execution on Ivanti Endpoint Manager Mobile (EPMM) servers through improper input validation.

New public exploit code

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

New critical CVEs

29

10.0 **CVE-2026-42826** Microsoft azure devops

Exposure of sensitive information to an unauthorized actor in Azure DevOps allows an unauthorized attacker to disclose information over a network.

9.9 **CVE-2026-33109** Microsoft azure managed instance for apache cassandra

+1 more CVEs in the same release

Improper access control in Azure Managed Instance for Apache Cassandra allows an authorized attacker to execute code over a network.

9.8 **CVE-2026-8091** Mozilla firefox

Incorrect boundary conditions in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 150, Thunderbird 150, Firefox ESR 140.10.1, Thunderbird 140.10.1, and Firefox ESR 115.35.2.

9.8 **CVE-2026-8094** Mozilla firefox

Other issue in the WebRTC component. This vulnerability was fixed in Firefox ESR 140.10.2 and Thunderbird 140.10.2.

9.8 **CVE-2026-8034** GitHub enterprise server

A server-side request forgery (SSRF) vulnerability was identified in the GitHub Enterprise Server notebook viewer that allowed an attacker to access internal services by exploiting URL parser confusion between the validation layer and the HTTP request library.

9.6 **CVE-2026-33823** Microsoft teams

Improper authorization in Microsoft Teams allows an authorized attacker to disclose information over a network.

9.6 **CVE-2026-35428** Microsoft azure cloud shell

Improper neutralization of special elements used in a command ('command injection') in Azure Cloud Shell allows an unauthorized attacker to perform spoofing over a network.

9.1 **CVE-2026-40982** Vmware spring cloud config

Spring Cloud Config allows applications to serve arbitrary text and binary files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack. Sprin

10.0 **CVE-2026-33587** Lfnovo open-notebook

Lack of user input sanitisation in Open Notebook v1.8.3 allows the application user to execute Python code (and subsequently OS commands) on the docker container via Server-Side Template Injection (SSTI) for user-created transformations.

9.8 **CVE-2026-42217** Openexr openexr

+1 more CVEs in the same release

OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From versions 3.0.0 to before 3.2.9, 3.3.0 to before 3.3.11, and 3.4.0 to before 3.4.11, readVariableLengthInteger(

9.8 **CVE-2026-41586** Hyperledger fabric

Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework for developing solutions and applications. From versions 1.0.0 to 2.2.26, Channel.java implements readObject() and exposes deSerializeChannel() which call ObjectInputStream.rea

9.8 **CVE-2026-6508**

Origin Validation Error vulnerability in TUBITAK BILGEM Software Technologies Research Institute Liderahenk allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Liderahenk: from 2.0.1 before 2.0.2.

9.8 **CVE-2026-30496**

The Optoma CinemaX P2 projector (firmware TVOS-04.24.010.04.01, Android 8.0.0) exposes an HTTP API on TCP port 2345 that allows full unauthenticated remote control of the device. The API supports both reading configuration (74 endpoints) and writing/modifying

9.8 **CVE-2025-63706**

NPM package next-npm-version1.0.1 is vulnerable to Command injection.

9.8 **CVE-2026-36458**

ChestnutCMS v1.5.10 has a SQL injection vulnerability. The content parameter of the cms_content tag can be manipulated in the admin backend and injected into a SQL query when the template is rendered.

9.8 **CVE-2025-63703**
npm package parse-ini v1.0.6 is vulnerable to Prototype Pollution in index.js().

9.8 **CVE-2025-63704**
NPM package query-parser-string 1.0.0 is vulnerable to Prototype Pollution. The package does not properly sanitize user supplied query parameters and merges them to the newly created object.

9.8 **CVE-2026-7414** Yarbo lawn mower firmware
Yarbo firmware v2.3.9 contains hardcoded administrative credentials embedded in the firmware image. These credentials are identical across all devices running this firmware and cannot be changed or removed by end users, enabling trivial unauthorized access to

9.8 **CVE-2026-7415** Yarbo lawn mower firmware
The MQTT broker embedded in Yarbo firmware v2.3.9 is configured to allow anonymous connections with no topic-level read or write ACLs. Any host on the same network can subscribe to sensitive telemetry topics or publish control messages directly to the robot wi

9.8 **CVE-2026-37709** Snipeitapp snipe-it
Insecure Permissions vulnerability in grokability snipe-it v.8.4.0 and before and fixed after 2026-03-10 commit 676a9958 allows a remote attacker to execute arbitrary code via the app/Http/Controllers/Api/UploadedFilesController.php component

7 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Woflow woflow.com 447,593 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.