Daily brief, Tuesday, April 14, 2026

Apr 13, 8:00 PM to Apr 14, 8:00 PM ET

Generated Nov 7, 2026, 7:11 AM ET

0	2	0	32	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 32 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.8 **CVE-2009-0238** Microsoft Office CISA KEV

Remote code execution in Microsoft Office Excel gives an attacker full system control when a user opens a crafted Excel file with a malformed object.

6.5 **CVE-2026-32201** Microsoft SharePoint Server CISA KEV

An attacker gains unauthorized access to sensitive information in Microsoft SharePoint Server through improper input validation.

New public exploit code

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

New critical CVEs

32

9.8 **CVE-2026-39813** Fortinet fortisandbox DETECTION

A path traversal: '../filedir' vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8 may allow attacker to escalation of privilege via specially crafted HTTP requests.

9.3 **CVE-2026-35033** Jellyfin jellyfin

Product not on watchlist.

10.0 **CVE-2026-39906** Unisys webperfect image suite

Unisys WebPerfect Image Suite versions 3.0.3960.22810 and 3.0.3960.22604 expose a deprecated .NET Remoting TCP channel that allows remote unauthenticated attackers to leak NTLMv2 machine-account hashes by supplying a Windows UNC path as a target file argument

10.0 **CVE-2026-39907** Unisys webperfect image suite

Unisys WebPerfect Image Suite versions 3.0.3960.22810 and 3.0.3960.22604 expose an unauthenticated WCF SOAP endpoint on TCP port 1208 that accepts unsanitized file paths in the ReadLicense action's LFName parameter, allowing remote attackers to trigger SMB con

9.9 **CVE-2026-27681**

Due to insufficient authorization checks in SAP Business Planning and Consolidation and SAP Business Warehouse, an authenticated user can execute crafted SQL statements to read, modify, and delete database data. This leads to a high impact on the confidentiali

9.9 **CVE-2026-38526**

An authenticated arbitrary file upload vulnerability in the /admin/tinymce/upload endpoint of Webkul Krayin CRM v2.2.x allows attackers to execute arbitrary code via uploading a crafted PHP file.

9.9 **CVE-2026-35031** Jellyfin jellyfin

Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chain in the subtitle upload endpoint (POST /Videos/{itemId}/Subtitles), where the Format field is not validated, allowing path traversal via the file extens

9.8 **CVE-2026-6264**

A critical vulnerability in the Talend JobServer and Talend Runtime allows unauthenticated remote code execution via the JMX monitoring port. The attack vector is the JMX monitoring port of the Talend JobServer. The vulnerability can be mitigated for the Talen

9.8 **CVE-2026-40288** Praison praisonai

PraisonAI is a multi-agent teams system. In versions below 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents, the workflow engine is vulnerable to arbitrary command and code execution through untrusted YAML files. When praisonai workflow run <file.yaml> load

9.8 **CVE-2026-40315** Praison praisonai

PraisonAI is a multi-agent teams system. Prior to 4.5.133, there is an SQL identifier injection vulnerability in SQLiteConversationStore where the table_prefix configuration value is directly concatenated into SQL queries via f-strings without any validation o

9.8 **CVE-2026-31049**

An issue in Hostbill v.2025-11-24 and 2025-12-01 allows a remote attacker to execute arbitrary code and escalate privileges via the CSV registration field

9.8 **CVE-2025-61260**

A vulnerability was identified in OpenAI Codex CLI v0.23.0 and before that enables code execution through malicious MCP (Model Context Protocol) configuration files. The attack is triggered when a user runs the codex command inside a malicious or compromised r

9.8 **CVE-2025-63939**

Improper input handling in /Grocery/search_products_itname.php, in anirudhkannan Grocery Store Management System 1.0, allows SQL injection via the sitem_name POST parameter.

9.8 **CVE-2025-65133**

A SQL injection vulnerability exists in the School Management System (version 1.0) by manikandan580. An unauthenticated or authenticated remote attacker can supply a crafted HTTP request to the affected endpoint to manipulate SQL query logic and extract sensit

9.8 **CVE-2025-65135**

In manikandan580 School-management-system 1.0, a time-based blind SQL injection vulnerability exists in /studentms/admin/between-date-reprtsdetails.php through the fromdate POST parameter.

9.8 **CVE-2025-70023**

An issue pertaining to CWE-843: Access of Resource Using Incompatible Type was discovered in transloadit uppy v0.25.6.

9.6 **CVE-2026-27303** Adobe connect

+1 more CVEs in the same release

Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a

9.6 **CVE-2026-39399**

NuGet Gallery is a package repository that powers nuget.org. A security vulnerability exists in the NuGetGallery backend job's handling of .nuspec files within NuGet packages. An attacker can supply a crafted nuspec file with malicious metadata, leading to cro

9.3 **CVE-2026-27243** Adobe connect

+1 more CVEs in the same release

Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over

9.3 **CVE-2026-27246** Adobe connect

Adobe Connect versions 2025.3, 12.10 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over

10 more critical CVEs in this window: see the dashboard

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.