Daily brief, Tuesday, April 21, 2026

Apr 20, 8:00 PM to Apr 21, 8:00 PM ET

Generated Nov 7, 2026, 6:01 AM ET

0	0	0	38	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

38 new critical CVEs.

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

38

9.8 **CVE-2026-6748** Mozilla firefox

Uninitialized memory in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.

9.8 **CVE-2026-6760** Mozilla firefox

+1 more CVEs in the same release

Mitigation bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.

9.8 **CVE-2026-6771** Mozilla firefox

Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.

9.8 **CVE-2026-34275** Oracle advanced inbound telephony

Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: Setup and Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with netw

9.6 **CVE-2026-5845** GitHub enterprise server

An improper authorization vulnerability in scoped user-to-server (ghu_) token authorization in GitHub Enterprise Server allows an authenticated attacker to access private repositories outside the intended installation scope, which can include write operations,

9.1 **CVE-2026-40372** Microsoft asp.net core

Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network.

9.1 **CVE-2026-34279** Oracle enterprise manager base platform

Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with netwo

9.1 **CVE-2026-34285** Oracle identity manager connector

+2 more CVEs in the same release

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS t

9.4 **CVE-2026-21571** Atlassian Bamboo Data Center

Product not on watchlist.

10.0 **CVE-2026-39861** Anthropic claude code

Claude Code is an agentic coding tool. Prior to version 2.1.64, Claude Code's sandbox did not prevent sandboxed processes from creating symlinks pointing to locations outside the workspace. When Claude Code subsequently wrote to a path within such a symlink, i

10.0 **CVE-2017-20230** Nwclark storable

Storable versions before 3.05 for Perl has a stack overflow. The retrieve_hook function stored the length of the class name into a signed integer but in read operations treated the length as unsigned. This allowed an attacker to craft data that could trigger t

10.0 **CVE-2025-15638** Atrodo net\

Net::Dropbear versions before 0.14 for Perl contains a vulnerable version of libtomcrypt. Net::Dropbear versions before 0.14 includes versions of Dropbear 2019.78 or earlier. These include versions of libtomcrypt v1.18.1 or earlier, which is affected by CVE-20

10.0 **CVE-2026-40911** Wwbn avideo

WWBN AVideo is an open source video platform. In versions 29.0 and prior, the YPTSocket plugin's WebSocket server relays attacker-supplied JSON message bodies to every connected client without sanitizing the `msg` or `callback` fields. On the client side, `plu

9.9 **CVE-2026-41329** Openclaw openclaw

OpenClaw before 2026.3.31 contains a sandbox bypass vulnerability allowing attackers to escalate privileges via heartbeat context inheritance and senderIsOwner parameter manipulation. Attackers can exploit improper context validation to bypass sandbox restrict

9.9 **CVE-2026-40906** Electric sync-service

Electric is a Postgres sync engine. From 1.1.12 to before 1.5.0, the order_by parameter in the ElectricSQL /v1/shape API is vulnerable to error-based SQL injection, allowing any authenticated user to read, write, and destroy the full contents of the underlying

9.9 **CVE-2026-40933** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, due to unsafe serialization of stdio commands in the MCP adapter, an authenticated attacker can add an MCP stdio server with an arbitrary command, achievin

9.8 **CVE-2026-5965**

NewSoftOA developed by NewSoft has an OS Command Injection vulnerability, allowing unauthenticated local attackers to inject arbitrary OS commands and execute them on the server.

9.8 **CVE-2026-40498** Freescout freescout

FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.213, an unauthenticated attacker can access diagnostic and system tools that should be restricted to administrators. The /system/cron endpoint relies on a static MD5 hash derive

9.8 **CVE-2026-38835** Tenda w30e firmware

Tenda W30E V2.0 V16.01.0.21 was found to contain a command injection vulnerability in the formSetUSBPartitionUmount function via the usbPartitionName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.

9.8 **CVE-2026-40050**

CrowdStrike has released security updates to address a critical unauthenticated path traversal vulnerability (CVE-2026-40050) in LogScale. This vulnerability only requires mitigation by customers that host specific versions of LogScale and does not affect Next

15 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.