Daily brief, Monday, April 20, 2026

Apr 19, 8:00 PM to Apr 20, 8:00 PM ET

Generated Nov 7, 2026, 6:11 AM ET

0	8	0	20	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

8 newly exploited, 20 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

8

10.0 **CVE-2025-32975** Quest KACE Systems Management Appliance (SMA) CISA KEV

Attackers can impersonate legitimate users and bypass authentication in Quest KACE Systems Management Appliance (SMA) without valid credentials.

8.2 **CVE-2023-27351** PaperCut NG/MF CISA KEV DETECTION

An attacker gains unauthorized administrative access and sensitive data in PaperCut NG and PaperCut MF through an improper authentication flaw.

7.5 **CVE-2026-20128** Cisco Catalyst SD-WAN Manager CISA KEV

A local, authenticated low-privileged user of Cisco Catalyst SD-WAN Manager can read a recoverable DCA user credential file and gain DCA user privileges.

7.3 **CVE-2024-27199** JetBrains TeamCity CISA KEV DETECTION

An attacker can read arbitrary files on JetBrains TeamCity servers through a relative path traversal flaw.

7.2 **CVE-2025-2749** Kentico Kentico Xperience CISA KEV

An authenticated Kentico Xperience user can upload arbitrary data to locations outside the intended path via path traversal in the Staging Sync Server.

6.5 **CVE-2026-20133** Cisco Catalyst SD-WAN Manager CISA KEV

Remote attackers can view sensitive information on systems running Cisco Catalyst SD-WAN Manager due to exposure to unauthorized actors.

6.1 **CVE-2025-48700** Synacor Zimbra Collaboration Suite (ZCS) CISA KEV

An attacker can inject malicious scripts into the Synacor Zimbra Collaboration Suite (ZCS) web interface, enabling session hijacking or data theft.

5.4 **CVE-2026-20122** Cisco Catalyst SD-WAN Manger CISA KEV

Cisco Catalyst SD-WAN Manager's API file handling flaw lets an attacker upload a malicious file to the local file system; the source summary is cut off before stating the resulting impact.

New public exploit code

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

New critical CVEs 20

10.0 **CVE-2025-32975** Quest KACE Systems Management Appliance (SMA) KEV

Attackers can impersonate legitimate users and bypass authentication in Quest KACE Systems Management Appliance (SMA) without valid credentials.

9.9 **CVE-2026-32604** Linuxfoundation spinnaker

Spinnaker is an open source, multi-cloud continuous delivery platform. In versions prior to 2026.1.0, 2026.0.1, 2025.4.2, and 2025.3.2, a bad actor can execute arbitrary commands very simply on the clouddriver pods. This can expose credentials, remove files, o

9.9 **CVE-2026-32613** Linuxfoundation spinnaker

Spinnaker is an open source, multi-cloud continuous delivery platform. Echo like some other services, uses SPeL (Spring Expression Language) to process information - specifically around expected artifacts. In versions prior to 2026.1.0, 2026.0.1, 2025.4.2, and

9.8 **CVE-2026-5963** Digiwin easyflow .net

+1 more CVEs in the same release

EasyFlow .NET developed by Digiwin has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

9.8 **CVE-2026-5450** Gnu glibc

Calling the scanf family of functions with a %mc (malloc'd character match) in the GNU C Library version 2.7 to version 2.43 with a format width specifier with an explicit width greater than 1024 could result in a one byte heap buffer overflow.

9.1 **CVE-2026-6257** Vvveb Vvveb CMS

Vvveb CMS before 1.0.8.2 contains a remote code execution vulnerability in its media management functionality where a missing return statement in the file rename handler allows authenticated attackers to rename files to blocked extensions .php or .htaccess. At

9.9 **CVE-2026-6643** Asustor data master

A stack-based buffer overflow vulnerability was found in the VPN Clients on the ADM. The issue stems from the use of unbounded sscanf() and passing user-controlled data directly to printf(). Due to the lack of PIE and Stack Canary protections, an authenticated

9.9 **CVE-2026-30269** Doorman doorman

Improper access control in Doorman v0.1.0 and v1.0.2 allows any authenticated user to update their own account role to a non-admin privileged role via /platform/user/{username}. The `role` field is accepted by the update model without a manage_users permission

9.8 **CVE-2026-32956** Silextechnology sd-330ac firmware

SD-330AC and AMC Manager provided by silex technology, Inc. contain a heap-based buffer overflow vulnerability in processing the redirect URLs. Arbitrary code may be executed on the device.

9.8 **CVE-2026-5760** Lmsys sglang

SGLang's reranking endpoint (/v1/rerank) achieves Remote Code Execution (RCE) when a model file containing a malcious tokenizer.chat_template is loaded, as the Jinja2 chat templates are rendered using an unsandboxed jinja2.Environment().

9.8 **CVE-2026-39918**

Vvveb prior to 1.0.8.1 contains a code injection vulnerability in the installation endpoint where the subdir POST parameter is written unsanitized into the env.php configuration file without escaping or validation. Attackers can inject arbitrary PHP code by br

9.8 **CVE-2026-29649** Xiangshan nemu

NEMU contains an implementation flaw in its RISC-V Hypervisor CSR handling where henvcfg[7:4] (CBIE/CBCFE/CBZE-related fields) is incorrectly masked/updated based on menvcfg[7:4], so a machine-mode write to menvcfg can implicitly modify the hypervisor's enviro

9.8 **CVE-2026-32311** Flowsint flowsint

Flowsint is an open-source OSINT graph exploration tool designed for cybersecurity investigation, transparency, and verification. Flowsint allows a user to create investigations, which are used to manage sketches and analyses. Sketches have controllable graphs

9.8 **CVE-2026-29646**

In OpenXiangShan NEMU prior to 55295c4, when running with RVH (Hypervisor extension) enabled, a VS-mode guest write to the supervisor interrupt-enable CSR (sie) may be handled incorrectly and can influence machine-level interrupt enable state (mie). This break

9.4 **CVE-2026-39109**

SQL Injection vulnerability in Apartment Visitors Management System Apartment Visitors Management System V1.1 within the username parameter of the login page (index.php). This allows an unauthenticated attacker to manipulate backend SQL queries during authenti

9.1 **CVE-2026-6644** Asustor data master

A command injection vulnerability was found in the PPTP VPN Clients on the ADM. The vulnerability allows an administrative user to break out of the restricted web environment and execute arbitrary code on the underlying operating system. This occurs due to ins

9.1 **CVE-2026-33557** Apache kafka

A possible security vulnerability has been identified in Apache Kafka. By default, the broker property `sasl.oauthbearer.jwt.validator.class` is set to `org.apache.kafka.common.security.oauthbearer.DefaultJwtValidator`. It accepts any JWT token without validat

9.1 **CVE-2026-33432** Roxy-Wi roxy-wi

Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions up to and including 8.2.8.2, when LDAP authentication is enabled, Roxy-WI constructs an LDAP search filter by directly concatenating the user-supplied login user

9.0 **CVE-2026-24467** Filigran openaev

OpenAEV is an open source platform allowing organizations to plan, schedule and conduct cyber adversary simulation campaign and tests. Starting in version 1.0.0 and prior to version 2.0.13, OpenAEV's password reset implementation contains multiple security wea

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.