Daily brief, Wednesday, March 18, 2026

Mar 17, 8:00 PM to Mar 18, 8:00 PM ET

Generated Nov 7, 2026, 11:48 AM ET

0	2	0	22	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 22 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.8 **CVE-2026-20963** Microsoft SharePoint CISA KEV

Untrusted data deserialization flaw in Microsoft SharePoint Server lets an attacker execute arbitrary code and gain elevated privileges.

7.2 **CVE-2025-66376** Synacor Zimbra Collaboration Suite (ZCS) CISA KEV

Attacker can execute arbitrary JavaScript in the Synacor Zimbra Collaboration Suite (ZCS) web interface, enabling session hijacking and data theft.

New public exploit code

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

New critical CVEs

22

9.8 **CVE-2026-20963** Microsoft SharePoint KEV

Untrusted data deserialization flaw in Microsoft SharePoint Server lets an attacker execute arbitrary code and gain elevated privileges.

9.8 **CVE-2026-25873**

OmniGen2-RL contains an unauthenticated remote code execution vulnerability in the reward server component that allows remote attackers to execute arbitrary commands by sending malicious HTTP POST requests. Attackers can exploit insecure pickle deserialization

9.8 **CVE-2026-30703**

A command injection vulnerability exists in the web management interface of the WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02). The adm.cgi endpoint improperly sanitizes user-supplied input provided to a command-related parameter in the sysCMD function

9.1 **CVE-2025-15031** Lfprojects mlflow

A vulnerability in MLflow's pyfunc extraction process allows for arbitrary file writes due to improper handling of tar archive entries. Specifically, the use of `tarfile.extractall` without path validation enables crafted tar.gz files containing `..` or absolu

9.8 **CVE-2026-27459** Pyopenssl pyopenssl

pyOpenSSL is a Python wrapper around the OpenSSL library. Starting in version 22.0.0 and prior to version 26.0.0, if a user provided callback to `set_cookie_generate_callback` returned a cookie value greater than 256 bytes, pyOpenSSL would overflow an OpenSSL

9.9 **CVE-2026-32731** Apostrophecms import-export

ApostropheCMS is an open-source content management framework. Prior to version 3.5.3 of `@apostrophecms/import-export`, The `extract()` function in `gzip.js` constructs file-write paths using `fs.createWriteStream(path.join(exportPath, header.name))`. `path.jo

9.1 **CVE-2026-31966** Htslib htslib

+1 more CVEs in the same release

HTSlib is a library for reading and writing bioinformatics file formats. CRAM is a compressed format which stores DNA sequence alignment data. As one method of removing redundant data, CRAM uses reference-based compression so that instead of storing the full s

9.8 **CVE-2026-31972** Samtools samtools

SAMtools is a program for reading, manipulating and writing bioinformatics file formats. The `mpileup` command outputs DNA sequences that have been aligned against a known reference. On each output line it writes the reference position, optionally the referenc

9.8 **CVE-2026-29859** Aapanel aapanel

An arbitrary file upload vulnerability in aaPanel v7.57.0 allows attackers to execute arbitrary code via uploading a crafted file.

9.1 **CVE-2026-32633** Nicolargo glances

Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.2, in Central Browser mode, the `/api/4/serverslist` endpoint returns raw server objects from `GlancesServersList.get_servers_list()`. Those objects are mutated in-place duri

10.0 **CVE-2026-32737** Ctfer-Io romeo

Romeo gives the capability to reach high code coverage of Go ?1.20 apps by helping to measure code coverage for functional and integration tests within GitHub Actions. Prior to version 0.2.1, due to a mis-written NetworkPolicy, a malicious actor can pivot from

9.1 **CVE-2026-30701**

The web interface of the WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) contains hardcoded credential disclosure mechanisms (in the form of Server Side Include) within multiple server-side web pages, including login.shtml and settings.shtml. These page

9.8 **CVE-2026-30702**
The WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) implements a broken authentication mechanism in its web management interface. The login page does not properly enforce session validation, allowing attackers to bypass authentication by directly access

9.8 **CVE-2026-25449**
Deserialization of Untrusted Data vulnerability in shinetheme Traveler traveler allows Object Injection.This issue affects Traveler: from n/a through < 3.2.8.1.

9.8 **CVE-2025-67830** Murasoftware mura cms
Mura before 10.1.14 allows beanFeed.cfc getQuery sortby SQL injection.

9.1 **CVE-2026-30704**
The WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02) exposes an unprotected UART interface through accessible hardware pads on the PCB

9.6 **CVE-2026-31938** Parall jspdf
jsPDF is a library to generate PDFs in JavaScript. Prior to version 4.2.1, user control of the `options` argument of the `output` function allows attackers to inject arbitrary HTML (such as scripts) into the browser context the created PDF is opened in. The vu

9.1 **CVE-2026-32698** Openproject openproject
OpenProject is an open-source, web-based project management software. Versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1 are vulnerable to an SQL injection attack via a custom field's name. When that custom field was used in a Cost Report, the custom field's

9.8 **CVE-2025-67829** Murasoftware mura cms
Mura before 10.1.14 allows beanFeed.cfc getQuery sortDirection SQL injection.

9.0 **CVE-2026-32703** Openproject openproject
OpenProject is an open-source, web-based project management software. In versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1, the Repositories module did not properly escape filenames displayed from repositories. This allowed an attacker with push access into

1 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Aura aura.com 903,080 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.