Daily brief, Monday, January 19, 2026

Jan 18, 7:00 PM to Jan 19, 7:00 PM ET

Generated Nov 7, 2026, 9:39 PM ET

0	0	0	18	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

18 new critical CVEs, 1 new breaches.

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

18

9.8 **CVE-2026-1162** Utt 810 firmware

A flaw has been found in UTT HiPER 810 1.7.4-141218. The impacted element is the function strcpy of the file /goform/setSysAdm. This manipulation of the argument passwd1 causes buffer overflow. Remote exploitation of the attack is possible. The exploit has bee

9.6 **CVE-2026-23852** B3log siyuan

SiYuan is a personal knowledge management system. Versions prior to 3.5.4 have a stored Cross-Site Scripting (XSS) vulnerability that allows an attacker to inject arbitrary HTML attributes into the `icon` attribute of a block via the `/api/attr/setBlockAttrs`

9.9 **CVE-2026-22797**

An issue was discovered in OpenStack keystonemiddleware 10.5 through 10.7 before 10.7.2, 10.8 and 10.9 before 10.9.1, and 10.10 through 10.12 before 10.12.1. The external_oauth2_token middleware fails to sanitize incoming authentication headers before processi

9.8 **CVE-2026-23837** Franklioxygen mytube

MyTube is a self-hosted downloader and player for several video websites. A vulnerability present in version 1.7.65 and poetntially earlier versions allows unauthenticated users to bypass the mandatory authentication check in the roleBasedAuthMiddleware. By si

9.8 **CVE-2026-23530** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0,`freerdp_bitmap_decompress_planar` does not validate `nSrcWidth`/`nSrcHeight` against `planar->maxWidth`/`maxHeight` before RLE decode. A malicious server can trigger a cl

9.8 **CVE-2026-23531** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, in ClearCodec, when `glyphData` is present, `clear_decompress` calls `freerdp_image_copy_no_overlap` without validating the destination rectangle, allowing an out-of-boun

9.8 **CVE-2026-23532** Freerdp freerdp

+2 more CVEs in the same release

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, a client-side heap buffer overflow occurs in the FreeRDP client's `gdi_SurfaceToSurface` path due to a mismatch between destination rectangle clamping and the actual copy

9.8 **CVE-2026-23944** Arcane arcane

Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to version 1.13.2, unauthenticated requests could be proxied to remote environment agents, allowing access to remote environment resources without authentication. The e

9.8 **CVE-2026-23883** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, `xf_Pointer_New` frees `cursorPixels` on failure, then `pointer_free` calls `xf_Pointer_Free` and frees it again, triggering ASan UAF. A malicious server can trigger a cl

9.8 **CVE-2026-23884** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.21.0, offscreen bitmap deletion leaves `gdi->drawing` pointing to freed memory, causing UAF when related update packets arrive. A malicious server can trigger a client?side use

9.9 **CVE-2026-23836** Hotcrp hotcrp

HotCRP is conference review software. A problem introduced in April 2024 in version 3.1 led to inadequately sanitized code generation for HotCRP formulas which allowed users to trigger the execution of arbitrary PHP code. The problem is patched in release vers

9.0 **CVE-2026-1181**

Altium 365 workspace endpoints were configured with an overly permissive Cross-Origin Resource Sharing (CORS) policy that allowed credentialed cross-origin requests from other Altium-controlled subdomains, including forum.live.altium.com. As a result, JavaScri

9.3 **CVE-2026-23839** Leepeuker movary

+2 more CVEs in the same release

Movary is a web application to track, rate and explore your movie watch history. Due to insufficient input validation, attackers can trigger cross-site scripting payloads in versions prior to 0.70.0. The vulnerable parameter is `?categoryUpdated=`. Version 0.7

9.8 **CVE-2026-0610** Devolutions devolutions server

SQL Injection vulnerability in remote-sessions in Devolutions Server.This issue affects Devolutions Server 2025.3.1 through 2025.3.12

Ransomware

No leak-site posts collected.

New data breaches 1

Raaga raaga.com 10,225,145 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.