Daily brief, Wednesday, April 22, 2026

Apr 21, 8:00 PM to Apr 22, 8:00 PM ET

Generated Nov 7, 2026, 5:51 AM ET

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

1 newly exploited, 18 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.8 **CVE-2026-33825** Microsoft Defender CISA KEV

An authorized local attacker can escalate privileges in Microsoft Defender due to insufficient access control granularity.

New public exploit code

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

New critical CVEs

18

9.8 **CVE-2026-31436** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix possible wrong descriptor completion in llist_abort_desc() At the end of this function, d is the traversal cursor of flist, but the code completes found instead. This can

9.8 **CVE-2026-31444** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free and NULL deref in smb_grant_oplock() smb_grant_oplock() has two issues in the oplock publication sequence: 1) opinfo is linked into ci->m_op_list (via opinfo_add) bef

9.8 **CVE-2026-31463** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: iomap: fix invalid folio access when i_blkbits differs from I/O granularity Commit aa35dd5cbc06 ("iomap: fix invalid folio access after folio_end_read()") partially addressed invalid folio acc

9.8 **CVE-2026-31478** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: replace hardcoded hdr2_len with offsetof() in smb2_calc_max_out_buf_len() After this commit (e2b76ab8b5c9 "ksmbd: add support for read compound"), response buffer management was changed

9.8 **CVE-2026-31501** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: ti: icssg-prueth: fix use-after-free of CPPI descriptor in RX path cppi5_hdesc_get_psdata() returns a pointer into the CPPI descriptor. In both emac_rx_packet() and emac_rx_packet_zc(), t

9.4 **CVE-2026-31448** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ext4: avoid infinite loops caused by residual data On the mkdir/mknod path, when mapping logical blocks to physical blocks, if inserting a new extent into the extent tree fails (in this exampl

9.8 **CVE-2026-41304** Wwbn avideo

WWBN AVideo is an open source video platform. In versions 29.0 and below, the `cloneServer.json.php` endpoint in the CloneSite plugin constructs shell commands using user-controlled input (`url` parameter) without proper sanitization. The input is directly con

9.8 **CVE-2026-6235**

The Sendmachine for WordPress plugin for WordPress is vulnerable to authorization bypass via the 'manage_admin_requests' function in all versions up to, and including, 1.0.20. This is due to the plugin not properly verifying that a user is authorized to perfor

9.8 **CVE-2018-25270** Thinkphp thinkphp

ThinkPHP 5.0.23 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by invoking functions through the routing parameter. Attackers can craft requests to the index.php endpoint with malicious functi

9.8 **CVE-2018-25272**

ELBA5 5.8.0 contains a remote code execution vulnerability that allows attackers to obtain database credentials and execute arbitrary commands with SYSTEM level permissions. Attackers can connect to the database using default connector credentials, decrypt the

9.8 **CVE-2026-34415**

Xerte Online Toolkits versions 3.15 and earlier contain an incomplete input validation vulnerability in the elFinder connector endpoint that fails to block PHP-executable extensions .php4 due to an incorrect regex pattern. Unauthenticated attackers can exploit

9.6 **CVE-2026-6356** Augmentt augmentt

A vulnerability in the web application allows standard users to escalate their privileges to those of a super administrator through parameter manipulation, enabling them to access and modify sensitive information.

9.6 **CVE-2026-33471** Nimiq nimiq proof-of-stake

nimiq-block contains block primitives to be used in Nimiq's Rust implementation. `SkipBlockProof::verify` computes its quorum check using `BitSet.len()`, then iterates `BitSet` indices and casts each `usize` index to `u16` (`slot as u16`) for slot lookup. Prio

9.3 **CVE-2026-41064** Wwbn avideo

WWBN AVideo is an open source video platform. In versions up to and including 29.0, an incomplete fix for AVideo's `test.php` adds `escapeshellarg` for wget but leaves the `file_get_contents` and `curl` code paths unsanitized, and the URL validation regex `/^h

9.1 **CVE-2026-40575** Oauth2 Proxy Project oauth2 proxy

OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions 7.5.0 through 7.15.1 may trust a client-supplied `X-Forwarded-Uri` header when `--reverse-proxy` is enabled and `--skip-auth-regex` or `--skip-auth-route` is configur

9.1 **CVE-2026-4119**

The Create DB Tables plugin for WordPress is vulnerable to authorization bypass in all versions up to and including 1.2.1. The plugin registers admin_post action hooks for creating tables (admin_post_add_table) and deleting tables (admin_post_delete_db_table)

9.1 **CVE-2026-33656** Espocrm espocrm

EspoCRM is an open source customer relationship management application. Prior to version 9.3.4, EspoCRM's built-in formula scripting engine allowing updating attachment's sourceId thus allowing an authenticated admin to overwrite the `sourceId` field on `Attac

9.1 **CVE-2026-41167**

Jellystat is a free and open source Statistics App for Jellyfin. Prior to version 1.1.10, multiple API endpoints in Jellystat build SQL queries by interpolating unsanitized request-body fields directly into raw SQL strings. An authenticated user can inject arb

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.