Daily brief, Thursday, May 28, 2026

May 27, 8:00 PM to May 28, 8:00 PM ET

Generated Nov 6, 2026, 11:00 PM ET

0	0	0	56	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

56 new critical CVEs, 2 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

56

9.4 **CVE-2026-32998** Veeam Service Provider Console

Product not on watchlist.

10.0 **CVE-2026-46840** Oracle rest data services

Vulnerability in Oracle REST Data Services (component: Backend-as-a-Service). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle REST Data

9.9 **CVE-2026-44477** Linuxfoundation cloudnativepg

CloudNativePG is a platform designed to manage PostgreSQL databases within Kubernetes environments. Prior to 1.29.1 and 1.28.3, the CloudNativePG metrics exporter opens its PostgreSQL connection as the postgres superuser via the pod-local Unix socket, then dem

9.9 **CVE-2026-46775** Oracle rest data services

+1 more CVEs in the same release

Vulnerability in Oracle REST Data Services (component: Core). Supported versions that are affected are 24.2.0-26.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle REST Data Services. While t

9.9 **CVE-2026-46822** Oracle iassets

Vulnerability in the Oracle iAssets product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to co

9.9 **CVE-2026-46824** Oracle universal work queue

Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker w

9.8 **CVE-2026-46115** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: block: add pgmap check to biovec_phys_mergeable biovec_phys_mergeable() is used by the request merge, DMA mapping, and integrity merge paths to decide if two physically contiguous bvec segment

9.8 **CVE-2026-46135** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fix race between ICReq handling and queue teardown nvmet_tcp_handle_icreq() updates queue->state after sending an Initialization Connection Response (ICResp), but it does so without

9.8 **CVE-2026-46137** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: ADD_ADDR rtx: fix potential data-race This mptcp_pm_add_timer() helper is executed as a timer callback in softirq context. To avoid any data races, the socket lock needs to be held

9.8 **CVE-2026-46195** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: validate dacloffset before building DACL pointers parse_sec_desc(), build_sec_desc(), and the chown path in id_mode_to_cifs_acl() all add the server-supplied dacloffset to pntsd b

9.8 **CVE-2026-34311** Oracle hospitality opera 5 property services

Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). Supported versions that are affected are 5.6.19.24, 5.6.22, 5.6.25.19, 5.6.27.6 and 5.6.28. Easily exploitable vulnerability allows

9.6 **CVE-2026-9872** Google chrome

Out of bounds write in GPU in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-9874** Google chrome

Use after free in Dawn in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-9875** Google chrome

Out of bounds read in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-9876** Google chrome
Use after free in WebGL in Google Chrome on Android prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-9886** Google chrome
Use after free in Base in Google Chrome on Mac prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-9918** Google chrome
Inappropriate implementation in Tint in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-9967** Google chrome
Out of bounds write in GPU in Google Chrome prior to 148.0.7778.216 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.1 **CVE-2026-46119** Linux linux kernel
In the Linux kernel, the following vulnerability has been resolved: libceph: Fix slab-out-of-bounds access in auth message processing If a (potentially corrupted) message of type CEPH_MSG_AUTH_REPLY contains a positive value in its result field, it is treated

9.1 **CVE-2026-46155** Linux linux kernel
In the Linux kernel, the following vulnerability has been resolved: smb/client: fix out-of-bounds read in smb2_compound_op() If a server sends a truncated response but a large OutputBufferLength, and terminates the EA list early, check_wsl_eas() returns succes

35 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 2

Charter charter.com 4,851,517 accounts

Kemper kemper.com 269,299 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.