Daily brief, Monday, May 4, 2026

May 3, 8:00 PM to May 4, 8:00 PM ET

Generated Nov 7, 2026, 3:36 AM ET

0	0	0	43	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

43 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

43

9.8 **CVE-2026-42238** Nginxui nginx ui

Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.8, nginx-ui exposes a backup restore endpoint (POST /api/restore) that is completely unauthenticated during the first 10 minutes after process startup on any fresh installation. An

9.8 **CVE-2026-7719** Totolink WA300

A security flaw has been discovered in Totolink WA300 5.2cu.7112_B20190227. The affected element is the function loginauth of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument http_host results in buffer over

9.8 **CVE-2026-7747** Totolink N300RH

A security flaw has been discovered in Totolink N300RH 3.2.4-B20220812. Affected by this vulnerability is the function loginauth of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. Performing a manipulation of the argument Password results in

9.9 **CVE-2026-29200** WebPros Comet Backup

A critical IDOR vulnerability has been discovered in Comet Backup affecting all versions from 20.11.0 to 26.1.1 and 26.2.1. The vulnerability allows a tenant administrator to impersonate any end-user account of other tenants on the same server via a vulnerable

10.0 **CVE-2026-42369**

GV-VMS V20 is a Video Monitoring Software used to gather the feeds of many surveillance cameras and manage other security devices. It is a native application accessed locally, but it is also possible to enable remote access via the "WebCam Server" feature. Onc

9.9 **CVE-2026-42364** Geovision gv-lpc2011 firmware

An os command injection vulnerability exists in the DdnsSetting.cgi functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted DDNS configuration can lead to arbitrary command execution. An attacker can modify a configuration value to trigger this vu

9.9 **CVE-2026-42368** Geovision gv-lpc2011 firmware

A privilege escalation vulnerability exists in the Web Interface functionality of GeoVision LPC2011/LPC2211 1.10. A specially crafted HTTP request can lead to execute priviledged operation. An attacker can visit a webpage to trigger this vulnerability.

9.9 **CVE-2026-42809** Apache polaris

Apache Polaris can issue broad temporary ("vended") storage credentials during staged table creation before the effective table location has been validated or durably reserved. Those temporary credentials are meant to limit the scope of accessible table data a

9.9 **CVE-2026-42810** Apache polaris

Apache Polaris accepts literal `*` characters in namespace and table names. When it later builds temporary S3 access policies for delegated table access, those same characters appear to be reused unescaped in S3 IAM resource patterns and `s3:prefix` conditions

9.9 **CVE-2026-42811** Apache polaris

In plain terms, Apache Polaris is supposed to issue short-lived GCS credentials that only work for one table's files, but a crafted namespace or table name can cause those credentials to work across the configured bucket instead. Apache Polaris builds Google C

9.9 **CVE-2026-42812** Apache polaris

In Apache Iceberg, the table's metadata files are control files: they tell readers which data files belong to the table and which table version to read. `write.metadata.path` is an optional table property that tells Polaris where to write those metadata files.

9.8 **CVE-2025-14320**

Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Tegsoft Management and Information Services Trade Limited Company Online Support Application allows Reflected XSS. This issue affects Online Support Applicati

9.8 **CVE-2025-70067**

Buffer Overflow vulnerability exists in Assimp versions up to 6.0.2 in the FBX Importer. The vulnerability occurs in aiMaterial::AddBinaryProperty, where a property key string from a crafted FBX file is copied into a fixed-size heap buffer using strcpy() witho

9.8 **CVE-2026-24118** Vm2 Project vm2

+1 more CVEs in the same release

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.0, VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue ha

9.8 **CVE-2026-24120** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.10.5, the fix for CVE-2023-37466 is insufficient and can be circumvented allowing attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system.

9.8 **CVE-2026-26332** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.0, SuppressedError allows attackers to escape the sandbox and run arbitrary code. This issue has been patched in version 3.11.0.

9.8 **CVE-2026-26956** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. In version 3.10.4, vm2 is vulnerable to full sandbox escape with arbitrary code execution. Attacker code inside VM.run() obtains host process object and runs host commands with zero host cooperation. This issue has

9.8 **CVE-2026-42027** Apache opennlp

Arbitrary Class Instantiation via Model Manifest in Apache OpenNLP ExtensionLoader Versions Affected: before 1.9.5, before 2.5.9, before 3.0.0-M3 Description: The ExtensionLoader.instantiateExtension(Class, String) method loads a class by its fully-qualified n

9.8 **CVE-2026-42076**

Evolver is a GEP-powered self-evolving engine for AI agents. Prior to version 1.69.3, a command injection vulnerability in the _extractLLM() function allows attackers to execute arbitrary shell commands on the server. The function constructs a curl command usi

9.8 **CVE-2026-42373** Dlink dir-605l firmware

D-Link DIR-605L Hardware Revision B2 (End-of-Life, EOL) contains a hardcoded telnet backdoor. The device starts a telnet daemon at boot via /bin/telnetd.sh with the username "Alphanetworks" and the static password "wrgn76_dlwbr_dir605L" read from /etc/alpha_co

22 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Reborn Gaming reborngaming.net 126 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.