Daily brief, Friday, June 5, 2026

Jun 4, 8:00 PM to Jun 5, 8:00 PM ET

Generated Nov 5, 2026, 7:24 AM ET

0	1	0	30	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 30 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.5 **CVE-2026-28318** SolarWinds Serv-U CISA KEV

An attacker can crash the Serv-U service without authentication.

New public exploit code

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

New critical CVEs

30

9.6 **CVE-2026-11250** Google chrome

Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security seve

9.6 **CVE-2026-11282** Google chrome

Insufficient policy enforcement in Sandbox in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)

9.6 **CVE-2026-11293** Google chrome

Use after free in Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)

10.0 **CVE-2026-49777** DETECTION

Improper Validation of Specified Quantity in Input vulnerability in ShapedPlugin, LLC Product Slider Pro for WooCommerce allows Malicious Software Implanted. This issue affects Product Slider Pro for WooCommerce: from n/a before 3.5.4.

10.0 **CVE-2026-46389** Defenseunicorns uds identity config

UDS Identity Config builds the Keycloak configuration image (realm, plugins, theme, truststore, JARs) consumed by UDS Core's Identity deployment. In versions 0.11.0 through 0.26.0, a logic error in the `client-kubernetes-secret` Keycloak client authenticator (

10.0 **CVE-2026-11429**

Two endpoints in the Vault Service ScriptsController, shared by Altium Enterprise Server and Altium 365, accept file uploads where a user-supplied filename component is used to construct the destination path without validation, allowing arbitrary files to be w

9.9 **CVE-2026-45744** Termix termix

+2 more CVEs in the same release

Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the GET /ssh/file_manager/ssh/resolvePath endpoint in Termix is vulnerable to OS command injection. The endpoint uses double-q

9.8 **CVE-2026-7762**

A heap-based buffer overflow vulnerability in the dot11ah.ko HaLow Wi-Fi kernel driver in Morse Micro HaLowLink 2 software versions prior to 2.11.13 allows an unauthenticated attacker within radio range to cause a Denial of Service (kernel panic) or potentiall

9.8 **CVE-2026-7763**

A heap-based buffer overflow vulnerability in the morse.ko HaLow Wi-Fi kernel driver in Morse Micro HaLowLink 2 software versions prior to 2.11.13 allows an unauthenticated attacker within radio range to cause a Denial of Service (kernel panic) or potentially

9.8 **CVE-2026-6274**

Improper Authentication, Missing authentication for critical function, Weak Authentication vulnerability in DTS Electronics Industry and Trade Ltd. Co. Redline WR3200 allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Redline W

9.8 **CVE-2026-10879** Perl dbi

DBI versions before 1.648 for Perl have a heap overflow when preparsing SQL statements with more than 9 binders. The preparse method expands SQL placeholder characters to numbered binders of the form :pN, but only allocates three characters per binder in the b

9.8 **CVE-2026-11362** Binary datadog\

DataDog::DogStatsd versions through 0.07 for Perl allow metric injections from event tags. DataDog::DogStatsd does not properly sanitise input, allowing metric injections of data from untrusted sources. The format_event method (used by the event method) does n

9.8 **CVE-2025-71317**

NetMan 204 contains a hard-coded backdoor account with the username and password 'eurek' that grants administrative access. A remote, unauthenticated attacker can authenticate through the cgi-bin/login.cgi endpoint (for example /cgi-bin/login.cgi?username=eure

9.8 **CVE-2025-71318**

NetMan 204 fails to enforce authentication on its administrative pages and command endpoints. A remote, unauthenticated attacker can directly request administrative pages (such as administration.html, administration-commands.html, and configuration.html) to di

9.8 **CVE-2026-45748** Termix termix

Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. The `POST /ssh/tunnel/connect` endpoint in Termix prior to version 2.3.2 builds an SSH tunnel command by interpolating user-controlled host record fie

9.8 **CVE-2026-10580** DETECTION

The Hippoo Mobile App for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to and including 1.9.4. This is due to a logic conflation in HippooPermissions::get_user_permissions(

9.8 **CVE-2026-11414** Altium on-prem enterprise server

A hard-coded cryptographic key is used by Altium Enterprise Server to sign file download URLs in the Vault service. Because the key is identical across all installations, an unauthenticated network attacker who can reach the server can forge valid download sig

9.8 **CVE-2026-11420** Altium on-prem enterprise server

Two path traversal vulnerabilities in the Network Installation Service (NIS) of Altium Enterprise Server allow an unauthenticated network attacker to write arbitrary files to any writable location on the server filesystem and to read package archive files from

9.8 **CVE-2026-45777** Buffalo open xdmod

OpenXDMoD is an open framework for collecting and analyzing HPC metrics. Starting in version 9.5.0 and prior to version 11.0.3, an attacker can remotely execute arbitrary system commands on the web server hosting Open XDMoD with the privileges of the web serve

9.8 **CVE-2026-45779** Buffalo open xdmod

OpenXDMoD is an open framework for collecting and analyzing HPC metrics. An SQL injection vulnerability exists in Open XDMoD versions prior to 10.0.3 that allows an unauthenticated remote attacker to execute arbitrary SQL statements. Exploitation requires no a

8 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

BCD Travel bcdtravel.com 396,313 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. CVE IDs link to the full record on Watch Floor.