Daily brief, Monday, June 29, 2026

Jun 28, 8:00 PM to Jun 29, 8:00 PM ET

Generated Nov 4, 2026, 7:48 AM ET

0	1	0	12	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 12 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-48558** SimpleHelp SimpleHelp CISA KEV DETECTION

An attacker can access remote support sessions on a SimpleHelp server without authentication.

New public exploit code

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

New critical CVEs

12

10.0 **CVE-2026-48558** SimpleHelp SimpleHelp KEV EXPLOIT CODE DETECTION

An attacker can access remote support sessions on a SimpleHelp server without authentication.

9.8 **CVE-2026-56290** Joomlack Page Builder KEV EXPLOIT CODE DETECTION

Joomla Extension - joomlack.fr - Unauthenticated file upload in Page Builder CK extension < 3.6.0 - The Joomla extension Page Builder CK is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE.

9.1 **CVE-2026-39868** Apple iOS and iPadOS

Product not on watchlist.

9.1 **CVE-2026-53434** Apache tomcat

Detection of Error Condition Without Action vulnerability in Apache Tomcat when configuring CRLs for a FFM based connector. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.22, from 10.1.0-M7 through 10.1.55, from 9.0.83 through 9.0.118. Users are

9.1 **CVE-2026-55276** Apache tomcat

Always-Incorrect Control Flow Implementation vulnerability in Apache Tomcat meant that special roles and empty authorisation constraints were not included when the effective web.xml was logged. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.22,

9.9 **CVE-2026-57331** Videowhisper Paid Videochat Turnkey Site

Performer Arbitrary File Deletion in Paid Videochat Turnkey Site <= 7.4.8 versions.

9.8 **CVE-2026-56782** DETECTION

Gorse before 0.5.10 contains an authentication bypass vulnerability in the /api/dump and /api/restore endpoints that allows unauthenticated attackers to access protected functionality when admin_api_key is empty, which is the default configuration. Remote atta

9.8 **CVE-2026-13762** Amazon cloudfront

Inconsistent interpretation of HTTP/2 requests in Amazon CloudFront with AWS WAF enabled might allow remote actors to bypass AWS WAF managed rule body inspection via crafted HTTP/2 requests that fragment the request body across frames so that only a partial bo

9.8 **CVE-2026-13763** Amazon application load balancer

Inconsistent interpretation of HTTP/2 requests in AWS Application Load Balancer with AWS WAF enabled might allow remote actors to bypass AWS WAF managed rule body inspection via crafted HTTP/2 requests that fragment the request body across frames so that only

9.6 **CVE-2026-57498**

Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, Coolify's API controllers consistently validate server ownership with Server::whereTeamId($teamId) before any operation. However, multi

9.1 **CVE-2026-11720** Google mcp toolbox for databases

A path traversal vulnerability exists in the HTTP tool URL builder of googleapis/mcp-toolbox. When constructing downstream API requests, the URL builder substitutes user-controlled pathParams into the configured tool path and parses the resulting string as a r

9.1 **CVE-2026-37637**

An issue in Alexantr filemanager v.1.0 allows a remote attacker to execute arbitrary code via the filemanager.php component

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. CVE IDs link to the full record on Watch Floor.