Daily brief, Friday, June 19, 2026

Jun 18, 8:00 PM to Jun 19, 8:00 PM ET

Generated Nov 4, 2026, 5:57 PM ET

0	0	0	29	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

29 new critical CVEs.

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

29

10.0 **CVE-2026-45480** Microsoft azure active directory

Improper authentication in Azure Active Directory allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-48584** Microsoft azure synapse

Execution with unnecessary privileges in Azure Synapse allows an authorized attacker to elevate privileges over a network.

9.6 **CVE-2026-48582** Microsoft exchange online

Missing authorization in Microsoft Exchange Online allows an authorized attacker to elevate privileges over a network.

10.0 **CVE-2026-50242** Jetbrains hub

In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 authentication bypass via direct database access leading to administrative access was possible

10.0 **CVE-2026-48772** Proxysql proxysql

ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. In versions 2.0.0 through 3.0.8, the ProxySQL MySQL frontend accepts the `PROXY UNKNOWN <addr> <addr> <port> <port>\r\n` PP1 frame as a well-formed PROXY protocol header. The HAProxy PROXY pro

9.9 **CVE-2026-56142** Jetbrains hub

In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 privilege escalation by attaching authentication details to accounts was possible

9.8 **CVE-2026-40624**

Improper input validation in AVer PTC500S, PTC115, PTC500+, and PTC115+ cameras may allow a remote, unauthenticated attacker to achieve arbitrary code execution via a specially crafted web request.

9.8 **CVE-2026-54414**

FileRise before 3.16.0 is vulnerable to path traversal in the shared-folder upload endpoint (/api/folder/uploadToSharedFolder.php), leading to arbitrary file write and administrator account takeover. The upload filename is validated by FolderController with ba

9.8 **CVE-2026-7515**

The BetterDocs Pro plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 3.8.0 via the `doc_style` parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server,

9.8 **CVE-2026-56141** Jetbrains hub

In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 account takeover via predictable restore codes was possible

9.8 **CVE-2026-51843** Tenda ac7 firmware

Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the wanMTU parameter.

9.8 **CVE-2026-51844** Tenda ac7 firmware

Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the cloneType parameter.

9.8 **CVE-2026-51845** Tenda ac7 firmware

Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the mac parameter.

9.8 **CVE-2026-51846** Tenda ac7 firmware

In Tenda AC7 v15.03.06.44, the wanSpeed parameter of the route /goform/AdvSetMacMtuWan has a stack buffer overflow vulnerability that can lead to remote arbitrary code execution.

9.8 **CVE-2026-48773** Proxysql proxysql

ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. Versions 2.0.18 through 3.0.8 have a pre-authentication heap memory corruption vulnerability in the MySQL and PostgreSQL protocol first-read paths. A remote unauthenticated client can declare

9.4 **CVE-2026-44939**

A command injection vulnerability in the Rancher Manager cluster before 2.14.2 import endpoint /v3/import/{token}_{clusterId}.yaml through unsanitized YAML parameters could allow remote attackers to break out of an image, and execute e.g. malicious containers.

9.4 **CVE-2026-56073**

Cap-go before 12.128.2 contains an authentication bypass vulnerability in OTP verification that allows attackers to bypass email verification by modifying server responses. Attackers can intercept OTP verification requests and manipulate HTTP responses to fals

9.3 **CVE-2026-12048** Pgadmin pgadmin 4

Stored cross-site scripting in pgAdmin 4's error-rendering and plan-node-rendering paths. Text returned by a PostgreSQL server (ErrorResponse messages, including object names quoted back inside relation-does-not-exist errors and inside EXPLAIN Recheck Cond / E

9.3 **CVE-2026-49871** Apache apisix

Cross-Site Request Forgery (CSRF) vulnerability in the cas-auth plugin under default configurations. This defect allows a remote attacker that manages to send a victim to a webpage controlled by them can cause the victim's browser to become authenticated as a

9.1 **CVE-2026-8713** DETECTION

The Avada (Fusion) Builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the maybe_delete_files function in all versions up to, and including, 3.15.3. This makes it possible for unauthenticated attack

9 more critical CVEs in this window: see the dashboard

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.