Daily brief, Wednesday, August 12, 2026

Aug 11, 8:00 PM to Aug 12, 8:00 PM ET

Generated Nov 2, 2026, 2:50 PM ET

0	0	0	52	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

52 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

52

9.8 **CVE-2026-26035** Fortinet fortiweb

An Improper Authentication vulnerability [CWE-287] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11, FortiWeb 7.2.0 through 7.2.12, FortiWeb 7.0.0 through 7.0.12 may allow a remote unauthentica

10.0 **CVE-2026-67282**

Joomla Extension - fabrikar.com - Unauthenticated remote code execution in Fabrik < 4.6.8 - An unauthenticated attacker could execute arbitrary code by using the frontend listfilter model.

10.0 **CVE-2026-73299**

Prompty is a markdown file format (.prompty) for LLM prompts. Prior to 0.1.5 and 2.0.0-beta.5, the TypeScript Nunjucks renderer evaluated untrusted .prompty template bodies with unrestricted JavaScript member access. An attacker-controlled template could trave

10.0 **CVE-2024-27253**

IBM DOORS Next 7.0.3 through 7.0.3 Interim Fix 018 could allow an authenticated user to bypass security logic to perform unauthorized activities.

9.9 **CVE-2026-72526**

A flaw was found in the multicloud-integrations component. The Application propagation controller processes the `ocm-managed-cluster` annotation from an Application Custom Resource (CR) without proper validation. A tenant with permissions to create Application

9.9 **CVE-2026-73263**

Prowler is a cloud security platform. Prior to 5.36.0, the Kubernetes provider connection test accepted kubeconfig_content containing a legacy gcp auth-provider with config.cmd-path and config.cmd-args because kubeconfig_contains_exec_auth in api/src/backend/a

9.9 **CVE-2026-73294**

Semaphore UI is a web interface for managing DevOps tools. Prior to 2.18.17 and 2.19.5-beta2, repository git_url handling passes an attacker-controlled --upload-pack option to CmdGitClient.GetLastRemoteCommitHash through POST /api/project/{id}/repositories and

9.9 **CVE-2026-16860** Ibm i

IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to an uncontrolled search path element.

9.9 **CVE-2026-19656** Scada-Lts scada-lts

ScadaLTS 2.7.8.1 exposes a server-side method that lacks authorization checks, allowing any authenticated user (including one holding only low-privilege, read-only permissions) to execute arbitrary operating system commands on the host. Successful exploitation

9.9 **CVE-2026-62420** Canonical lxd

An authorization bypass vulnerability in LXD allows an authenticated attacker to bypass target project security restrictions during cross-project instance migrations. When moving an instance cross-project to a different cluster member via POST /1.0/instances/{

9.9 **CVE-2026-63293** Canonical lxd

A link following vulnerability in LXD allows an attacker to achieve arbitrary file read and write operations on the host system. When importing or unpacking an image archive, LXD fails to validate whether the metadata.yaml file is a symbolic link. An attacker

9.9 **CVE-2026-63294** Canonical lxd

A link following vulnerability in LXD allows an attacker to achieve root command execution on the host system. During the import or unpacking of crafted image or backup archives, LXD fails to properly validate and confine the backup.yaml file when it exists as

9.9 **CVE-2026-63296** Canonical lxd

An authorization bypass vulnerability in LXD allows an authenticated attacker to bypass target project restrictions during instance migration. When migrating an instance to a target project, LXD accepts configuration overrides without validating the new config

9.9 **CVE-2026-63297** Canonical lxd

An authorization bypass vulnerability in LXD due to a timing flaw during configuration merging allows an authenticated attacker to bypass target project restrictions during cross-project instance copies. When copying an instance to a target project, LXD perfor

9.9 **CVE-2026-63298** Canonical lxd

An improper neutralization of special elements vulnerability in LXD's NVIDIA instance configuration handling allows an authenticated attacker to inject arbitrary configuration directives. By supplying newline characters within the 'nvidia.driver.capabilities'

9.9 **CVE-2026-63299** Canonical lxd

An authorization bypass vulnerability in LXD allows an authenticated user to bypass project-level disk and volume limits. Two related code paths fail to verify resource limits during volume operations: the storagePoolVolumeTypePostMove function omits the limit

9.9 **CVE-2026-63300** Canonical lxd

An improper validation vulnerability in the instancePostMigration function in lxd/instance_post.go of LXD allows an authenticated attacker with can_create_instances permissions on a restricted project to bypass project-level security restrictions. When migrati

9.9 **CVE-2026-72508**

A flaw was found in the multicloud-operators-subscription component of Red Hat Advanced Cluster Management (RHACM). This vulnerability allows a namespace-admin tenant to perform a confused-deputy attack by creating Subscription Custom Resources (CRs) that leve

9.9 **CVE-2026-73268**

A flaw was found in the cluster-curator-controller component of multicluster engine (MCE). A tenant with create or update permissions on ClusterCurator resources can inject an arbitrary Job specification. This is possible because the CreateJob() function does

9.9 **CVE-2026-73269**

A flaw was found in the cluster-curator-controller component. A local user, by creating a ClusterCurator resource with a specific naming convention, can trigger the creation of a cluster-scoped ClusterRoleBinding. This allows the user to escalate their privile

32 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.