Daily brief, Monday, June 22, 2026

Jun 21, 8:00 PM to Jun 22, 8:00 PM ET

Generated Nov 4, 2026, 2:57 PM ET

0	0	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

16 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

16

10.0 **CVE-2026-10561** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.9.3 has an vulnerability due to an improper isolation of Python execution combined with an authentication bypass that allows an unauthenticated attacker to execute arbitrary code on the host system, resulting in complete compro

9.8 **CVE-2026-7664** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.8.4 could allow unauthenticated attackers to access protected MCP project resources and execute MCP operations due to improper authorization enforcement in the Streamable MCP transport endpoint.

9.8 **CVE-2026-49468** Litellm litellm DETECTION

LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.84.0, a Host-header parsing flaw in the LiteLLM proxy could, under specific conditions, allow unauthenticated access to protected management routes. The auth layer

9.6 **CVE-2026-28381** Grafana snowflake

The Snowflake datasource allows for GET/PUT commands, which can allow any user with access to run queries against the data source to read/write files between the local grafana server and the connected Snowflake host.

9.6 **CVE-2026-10789** Autodesk fusion

A maliciously crafted webpage, when visited by a user with Autodesk Fusion Desktop running and the MCP extension enabled, can trigger a vulnerability in the MCP extension that could allow arbitrary code execution. A successful exploit may allow code to execute

9.4 **CVE-2026-11746**

A vulnerability has been identified in centraldogma-server versions prior to 0.84.0, where enabling ZooKeeper replication without setting replication.secret causes the server to silently fall back to a hard-coded, publicly known secret. This default credential

9.4 **CVE-2026-56422**

Multiple MISP core controllers and model capture paths accepted client-controlled request fields such as primary keys (id) and ownership/scope foreign keys (event_id, org_id, user_id, sharing_group_id, galaxy_cluster_uuid, organisation_uuid, and related nested

9.4 **CVE-2026-7165**

The vulnerability is present in the ‘/addJugador’ endpoint: * The 'keyJugador' and 'keyJugadorObjectiu' parameters allow the modification of other users’ information without requiring prior authorization validation. This could enable an authenticated attacker

9.2 **CVE-2026-7166**

Vulnerability involving the exposure of sensitive data provided without adequate protection. The API exposes email and phone number data from the ‘email’ and ‘telefon’ fields. This vulnerability is also present in the local database, as it contains accessible

9.2 **CVE-2026-45034**

PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. Prior to 1.30.5, CVE-2026-34084 was patched by the helper File::prohibitWrappers. The helper calls parse_url($filename, PHP_URL_SCHEME) and then checks is_string($scheme) && strlen

9.1 **CVE-2026-11373**

Net::Statsite::Client versions through 1.1.0 for Perl allow metric injections. Net::Statsite::Client is a client for the statsite protocol, which is a variant of statsd. Newlines are not removed from metric names, allowing metric injections. Values are not san

9.1 **CVE-2026-12628** Ibm storage protect

IBM Storage Protect Client 8.1.0.0 through 8.2.1.0 and IBM Storage Protect Snapshot For Windows 8.1.0.0 through 8.2.1.0 could allow a remote attacker to bypass authentication due to the use of a hardcoded credential in the FlashCopy Manager (FCM) authenticatio

9.1 **CVE-2026-48509** Messagepack messagepack

MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, the parameterless MessagePackInputFormatter() constructor uses default serializer options, which resolve to MessagePackSerializerOptions.Standard with MessagePackSecurity.Truste

9.1 **CVE-2026-56348** N8n n8n

n8n before 2.20.0 contains a credential exfiltration vulnerability in the POST /rest/dynamic-node-parameters/options endpoint that allows authenticated users to bypass Allowed HTTP Request Domains restrictions. Attackers with credential access can cause the n8

9.1 **CVE-2026-48746** Vllm vllm

vLLM is an inference and serving engine for large language models (LLMs). From 0.3.0 until 0.22.0, a vulnerability in ASGI web servers and starlette's trust on those web servers enables an authentication bypass of the OpenAI API AuthenticationMiddleware. It al

9.0 **CVE-2026-12249**

An issue was discovered in Canonical ADSys upstream versions through v0.16.2. During Active Directory Certificate Services (AD CS) certificate auto-enrollment via the vendored Samba client script (internal/policies/certificate/python/vendor_samba/gp/gp_cert_au

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.