Daily brief, Thursday, August 27, 2026

Aug 26, 8:00 PM to Aug 27, 8:00 PM ET

Generated Nov 2, 2026, 1:14 AM ET

0	3	0	54	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 54 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

9.8 **CVE-2023-49105** ownCloud ownCloud CISA KEV DETECTION

An attacker can access, modify, or delete any file without authentication on ownCloud.

7.8 **CVE-2026-53362** Linux Kernel CISA KEV

An attacker can escalate privileges via IPv6 networking on Linux Kernel.

5.3 **CVE-2026-66384** JFrog Artifactory CISA KEV

An authenticated attacker gains ability to write data outside the intended Docker cache path on JFrog Artifactory.

New public exploit code

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

New critical CVEs

54

9.8 **CVE-2023-49105** ownCloud ownCloud KEV EXPLOIT CODE DETECTION

An attacker can access, modify, or delete any file without authentication on ownCloud.

9.8 **CVE-2026-47884** Vmware spring framework

Use of XsltView in a Spring MVC application can result in SSRF and RCE attack if the application has an "/**" mapping that results in view rendering, and where the view name is not explicitly specified. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6

9.8 **CVE-2026-47890** Vmware spring framework

Spring MVC and WebFlux applications are vulnerable to stream corruption when using Server-Sent Events (SSE) with view fragments. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19

9.8 **CVE-2026-47891** Vmware spring framework

A Spring WebFlux application that relies on the Aalto XML processor to parse XML input does not correctly enforce the maxInMemorySize limit. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 -

9.8 **CVE-2026-47892** Vmware spring framework

A WebFlux application using functional endpoints and deployed with DispatcherServlet may be vulnerable to a header predicate bypass in a pre-flight request. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring F

9.8 **CVE-2026-81700** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.9 contain a signature verification vulnerability in gpg_runner.verify_detached that accepts revoked and expired keys by only checking VALIDSIG status without inspecting REVKEYSIG, EXPKEYSIG, or gpg exit codes. Attackers hold

9.8 **CVE-2026-81701** Jahlives openssl encrypt

openssl_encrypt versions before 1.4.9 use a denylist to identify trusted built-in plugins, allowing unsigned plugins in top-level plugins/ directories and unknown subdirectories to bypass signature verification. Attackers can place malicious unsigned plugins f

9.8 **CVE-2026-81702** Jahlives openssl encrypt

openssl_encrypt before 1.4.9 fails to re-derive and validate fingerprints when loading identities from identity.json, allowing attackers to substitute public keys in identity stores. Attackers can replace legitimate public keys with their own while maintaining

9.8 **CVE-2026-59313** Vmware spring framework

Spring MVC applications using the functional web framework are vulnerable to stream corruption when using Server-Sent Events (SSE). Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 S

9.6 **CVE-2026-59354** Vmware spring security

In versions of Spring Security's OAuth2 Authorization Server module 7.0.0 through 7.0.4, when Dynamic Client Registration is explicitly enabled, the registration endpoint performs insufficient validation of certain client metadata fields supplied by the regist

9.4 **CVE-2026-59270** Vmware spring security

Spring Security's embedded UnboundID LDAP server (UnboundIdContainer) unconditionally registers an administrative credential and binds its listener to all available network interfaces. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 -

9.1 **CVE-2026-59283** Vmware spring framework

Applications that evaluate Spring Expression Language (SpEL) expressions using SimpleEvaluationContext may be vulnerable to a safety guard bypass when the SpEL expression compiler is active. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring

9.8 **CVE-2026-30612**
Product not on watchlist.

10.0 **CVE-2026-81096**
ToolUniverse ran caller-supplied Python inside a sandbox that could be escaped, on a server that required no authentication. The executor behind the python_code_executor tool, in python_executor_tool.py, inspected the submitted source for a denied list of attr

10.0 **CVE-2026-81735**
startServer.ts in the mcp-http-server package of UI-TARS-desktop defaulted its listen address to '::' when no host was given, so startSseAndStreamableHttpMcpServer bound the Streamable HTTP and SSE MCP transports to every interface, and its authentication midd

10.0 **CVE-2026-18885**
ServiceNow has remediated a code injection vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute arbitrary code in the ServiceNow platform and gain access

10.0 **CVE-2026-18886**
ServiceNow has remediated an improper access control vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to create or modify instance data beyond what was intended,

10.0 **CVE-2026-6876**
ServiceNow has remediated a sandbox escape security issue that was identified in the ServiceNow AI Platform. This security issue could allow an unauthenticated user to execute arbitrary code within the ServiceNow AI Platform, potentially leading to more access

10.0 **CVE-2026-74820**
ServiceNow has remediated a SQL injection vulnerability that was identified in in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute arbitrary SQL statements against the instance's underlyi

9.8 **CVE-2026-32566**
Unauthenticated Privilege Escalation in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.

34 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.