Daily brief, Tuesday, August 4, 2026

Aug 3, 8:00 PM to Aug 4, 8:00 PM ET

Generated Nov 2, 2026, 10:44 PM ET

0	3	0	44	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 44 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

9.8 **CVE-2026-9198** IBM Langflow CISA KEV DETECTION

An attacker gains full remote code execution on IBM Langflow without authentication.

8.2 **CVE-2026-18556** N-able N-central CISA KEV

An attacker can bypass authentication in N-able N-central.

7.5 **CVE-2026-34486** Apache Tomcat CISA KEV DETECTION

An attacker bypasses encryption with Apache Tomcat.

New public exploit code

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

New critical CVEs

44

9.8 **CVE-2026-9198** IBM Langflow KEV EXPLOIT CODE DETECTION

An attacker gains full remote code execution on IBM Langflow without authentication.

9.8 **CVE-2026-63455** Hewlett Packard Enterprise (HPE) EdgeConnect SD-WAN Orchestrator

+1 more CVEs in the same release

Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view

10.0 **CVE-2026-64633** Veeam ONE

A vulnerability allowing remote unauthenticated code execution on the agent host.

9.0 **CVE-2026-58072** Veeam Service Provider Console

A vulnerability in Veeam Service Provider Console allowing arbitrary file write on the management server, which can lead to remotecode execution.

9.5 **CVE-2026-58073** Veeam Service Provider Console

A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to impersonate a managed agent andobtain that agent's credentials.

9.8 **CVE-2026-0163** Google android

In multiple functions of vpu_ioctl.c, there is a possible use after free due to a use after free. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

9.8 **CVE-2026-24254** Nvidia dynamo

NVIDIA Dynamo for Linux contains a vulnerability in the multimodal serving topology, where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial

9.1 **CVE-2026-69258** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the unauthenticated POST /api/v1/prediction/:id endpoint accepted an overrideConfig object and unconditionally spread it into internal flowConfig and flowD

9.8 **CVE-2026-69263** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the mitigation for CVE-2025-8943 blocked -y and --yes flags on npx, but packages/components/nodes/tools/MCP/core.ts denied only PATH, LD_LIBRARY_PATH, DYLD

10.0 **CVE-2026-70478** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.3, the POST /api/v1/oauth2-credential/refresh/:credentialId endpoint is included in WHITELIST_URLS and requires no authentication. The endpoint decrypts the s

9.8 **CVE-2026-18685**

A security vulnerability has been detected in GL.iNet GL-MT3000 up to 4.4.5. Impacted is the function set_upgrade of the file /cgi-bin/glc of the component modem.so. Such manipulation leads to command injection. It is possible to launch the attack remotely. Th

9.8 **CVE-2026-18686**

A vulnerability was detected in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function nas-web.add_user of the file /cgi-bin/glc of the component nas-web RPC Wrapper. Performing a manipulation results in command injection. The attack can be initia

9.8 **CVE-2026-16618**

The Improve SEO WordPress plugin through 2.0.11 does not properly validate uploaded files, checking only the file content type while writing the file with the attacker-supplied extension into a publicly accessible directory, allowing unauthenticated users to u

9.8 **CVE-2026-64564**

In the Linux kernel, the following vulnerability has been resolved: sctp: don't free the ASCONF's own transport in DEL-IP processing sctp_process_asconf() caches the transport the ASCONF chunk is processed against in asconf->transport (== chunk->transport, set

9.8 **CVE-2026-14175**

Unrestricted upload of file with dangerous type vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Upload a Web Shell to a Web Server. This issue affects HUMANIST Digital Human Resources: from 26.0 before 2

9.8 **CVE-2026-15721**

Cleartext storage of sensitive information vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows SQL Injection. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.

9.8 **CVE-2026-61514**

Puwell IP Camera firmware versions 2.x through 4.x contains an authentication bypass vulnerability that allows unauthenticated attackers to access device functions by sending protocol-conforming packets over TCP port 23456 without credentials. Attackers can ex

9.8 **CVE-2026-61515**

Puwell IP Camera firmware versions 2.x through 4.x contains an unauthenticated command injection vulnerability that allows remote attackers to execute arbitrary operating system commands by sending a crafted JSON payload to the DebugShell interface exposed on

9.8 **CVE-2026-69098**

kotaemon through 0.12.0 contains an insecure deserialization vulnerability in the check_connection endpoint that allows unauthenticated attackers to instantiate arbitrary Python classes by supplying crafted YAML/JSON input with a __type__ field. Attackers can

9.8 **CVE-2025-29296**

H3C Magic BE18000 V200R007, H3C NX400 V100R015, H3C Magic NX30 Pro V100R0011, H3C Magic R3010 V100R009, H3C Magic NX15 V100R017, H3C Magic R1510 V100R016, H3C NE36 Pro V100R002 and H3C MC102G HM1A0V200R010 contain multiple command injection vulnerabilities in

23 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.