Daily brief, Tuesday, May 26, 2026

May 25, 8:00 PM to May 26, 8:00 PM ET

Generated Nov 6, 2026, 11:05 PM ET

0	1	0	33	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 33 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-48172** LiteSpeed cPanel Plugin CISA KEV

Any cPanel user account can execute arbitrary scripts with root privileges via the LiteSpeed cPanel Plugin, a privilege escalation flaw.

New public exploit code

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

New critical CVEs

33

10.0 **CVE-2026-48172** LiteSpeed cPanel Plugin KEV EXPLOIT CODE

Any cPanel user account can execute arbitrary scripts with root privileges via the LiteSpeed cPanel Plugin, a privilege escalation flaw.

9.9 **CVE-2026-7374**

A flaw was found in KubeVirt's virt-handler component. This vulnerability allows an authenticated OpenShift user with edit permissions in a single namespace to exploit improper symlink validation when connecting to virtual machine console sockets. By replacing

9.9 **CVE-2026-46624** Twenty twenty

Twenty is an open source CRM. From 1.7.7 through 1.16.7, a critical Remote Code Execution (RCE) vulnerability exists in Twenty CRM via a chained SQL Injection and PostgreSQL COPY TO PROGRAM attack. If Postgres user is a super user then any authenticated user c

9.9 **CVE-2026-44450**

Lumiverse is a full-featured AI chat application. Prior to 0.9.7, the MCP server creation endpoint validates the command field against an allowlist of binary names but forwards the args array to the child process without any validation. Every binary on the all

9.8 **CVE-2026-8376** Perl perl

Perl versions before 5.40.5-RC1, from 5.41.0 before 5.42.3-RC1, from 5.43.0 before 5.43.11 have a heap buffer overflow when compiling regular expressions with a repeated fixed string on 32-bit builds. Perl_study_chunk in regcomp_study.c checked the size of the

9.8 **CVE-2026-9543** DETECTION

A vulnerability has been found in Totolink N300RH 6.1c.1353_B20190305. Affected is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument admpass leads to os command injection.

9.8 **CVE-2026-48686** Pavel-Odintsov fastnetmon

FastNetMon Community Edition through 1.2.9 contains a stack-based buffer overflow in the BGP NLRI (Network Layer Reachability Information) decoder. The function decode_bgp_subnet_encoding_ipv4_raw() in src/bgp_protocol.cpp reads prefix_bit_length directly from

9.8 **CVE-2026-48687** Pavel-Odintsov fastnetmon

FastNetMon Community Edition through 1.2.9 contains an OS command injection vulnerability in the Juniper router integration plugin. The _log() function in src/juniper_plugin/fastnetmon_juniper.php (lines 117-118) constructs shell commands by concatenating the

9.8 **CVE-2026-35221** Joomla joomla\!

Improperly built filter clauses lead to a SQL injection vulnerability in the search query for com_finder.

9.8 **CVE-2026-35222** Joomla joomla\!

Improperly validated order clauses lead to a SQL injection vulnerability in com_tags.

9.8 **CVE-2026-35223** Joomla joomla\!

An improper access check allows unauthorized access to com_config webservice endpoints.

9.8 **CVE-2026-40383** Joomla joomla\!

An improper validation of user-supplied input leads to a local file inclusion vulnerability.

9.8 **CVE-2026-48691** Pavel-Odintsov fastnetmon

FastNetMon Community Edition through 1.2.9 contains an integer overflow in the BGP AS_PATH attribute encoder. In src/bgp_protocol.hpp, the IPv4UnicastAnnounce::get_attributes() function computes attribute_length as 'sizeof(bgp_as_path_segment_element_t) + this

9.8 **CVE-2026-48898** Joomla joomla\!

+1 more CVEs in the same release

An improper access check allows privilege escalation through the com_users batch task.

9.8 **CVE-2026-48902** Joomla joomla\!

The password and username reset features created plain http links for https connections if the "Force SSL" flag wasn't explicitly set.

9.8 **CVE-2026-48904** Joomla joomla\!
An improper access check allows privelege escalation through the com_users group editing webservice endpoint.

9.8 **CVE-2026-44668**
FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to 1.8.3, AccessControlInterceptor, the authentication gate for all Struts2 actions, unconditionally calls invocation.invoke() without checking for a valid session. Four action method

9.8 **CVE-2026-7251**
Eppendorf BioFlo 320 is vulnerable due to VNC server using a hard-coded password. If a remote attacker knows the network address of any BioFlo 320 model with remote access enabled, they can gain full control of the user interface by using this password. Once c

9.8 **CVE-2026-8633** Ibm websphere application server
IBM Web Server Plug-ins for WebSphere Application Server and WebSphere Liberty 8.5, 9.0 IBM WebSphere Application Server and WebSphere Application Server Liberty are vulnerable to remote code execution in the Web Server Plug-ins, through a specially crafted re

9.8 **CVE-2026-9170** Ibm http server
IBM HTTP Server 8.5, and 9.0 is vulnerable to denial of service and a potential remote code execution due to improper input validation.

12 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Ameriprise ameriprise.com FINANCE 502,597 accounts

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.