Daily brief, Wednesday, November 26, 2025

Nov 25, 7:00 PM to Nov 26, 7:00 PM ET

Generated Nov 9, 2026, 7:17 AM ET

0	0	0	30	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

30 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

30

9.8 **CVE-2025-64657** Microsoft azure application gateway

Stack-based buffer overflow in Azure Application Gateway allows an unauthorized attacker to elevate privileges over a network.

9.4 **CVE-2025-64656** Microsoft azure application gateway

Out-of-bounds read in Application Gateway allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2025-64126**

An OS command injection vulnerability exists due to improper input validation. The application accepts a parameter directly from user input without verifying it is a valid IP address or filtering potentially malicious characters. This could allow an unauthenti

10.0 **CVE-2025-64127**

An OS command injection vulnerability exists due to insufficient sanitization of user-supplied input. The application accepts parameters that are later incorporated into OS commands without adequate validation. This could allow an unauthenticated attacker to e

10.0 **CVE-2025-64128**

An OS command injection vulnerability exists due to incomplete validation of user-supplied input. Validation fails to enforce sufficient formatting rules, which could permit attackers to append arbitrary data. This could allow an unauthenticated attacker to in

9.8 **CVE-2025-66253** Dbbroadcast mozart next 100 firmware

Unauthenticated OS Command Injection (start_upgrade.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform User input passed directly to exec() allo

9.8 **CVE-2025-66261** Dbbroadcast mozart next 100 firmware

Unauthenticated OS Command Injection (restore_settings.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform URL-decoded name parameter passed to e

9.8 **CVE-2025-66262** Dbbroadcast mozart next 100 firmware

Arbitrary File Overwrite via Tar Extraction Path Traversal in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Tar extraction with -C / allow arbitrar

9.8 **CVE-2025-62354**

Improper neutralization of special elements used in an OS command ('command injection') in Cursor allows an unauthorized attacker to execute commands that are outside of those specified in the allowlist, resulting in arbitrary code execution.

9.8 **CVE-2025-64130**

Zenitel TCIV-3+ is vulnerable to a reflected cross-site scripting vulnerability, which could allow a remote attacker to execute arbitrary JavaScript on the victim's browser.

9.6 **CVE-2025-66022** Owasp faction

FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to version 1.7.1, an extension execution path in Faction’s extension framework permits untrusted extension code to execute arbitrary system commands on the server when a lifecycle hoo

9.8 **CVE-2025-66259** Dbbroadcast mozart next 100 firmware

Authenticated Root Remote Code Execution via improrer user input filtering in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform in main_ok.php user sup

9.8 **CVE-2025-59390** Apache druid

Apache Druid’s Kerberos authenticator uses a weak fallback secret when the `druid.auth.authenticator.kerberos.cookieSignatureSecret` configuration is not explicitly set. In this case, the secret is generated using `ThreadLocalRandom`, which is not a crypto-gra

9.8 **CVE-2025-26155** Ncp-E ncp secure entry client

NCP Secure Enterprise Client 13.18 and NCP Secure Entry Windows Client 13.19 have an Untrusted Search Path vulnerability.

9.1 **CVE-2025-66251** Dbbroadcast mozart next 100 firmware

Unauthenticated Path Traversal with Arbitrary File Deletion in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform The deletehidden parameter allows path

9.1 **CVE-2025-65669** Classroomio classroomio

An issue was discovered in classroomio 0.1.13. Student accounts are able to delete courses from the Explore page without any authorization or authentication checks, bypassing the expected admin-only deletion restriction.

9.8 **CVE-2025-65235** Opencode ussd gateway

OpenCode Systems USSD Gateway OC Release: 5 Version 6.13.11 was discovered to contain a SQL injection vulnerability via the ID parameter in the getSubUsersByProvider function.

9.8 **CVE-2025-65236** Opencode ussd gateway

OpenCode Systems USSD Gateway OC Release: 5 was discovered to contain a SQL injection vulnerability via the Session ID parameter in the /occontrolpanel/index.php endpoint.

9.8 **CVE-2025-66250** Dbbroadcast mozart next 100 firmware

Unauthenticated Arbitrary File Upload (status_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Allows unauthenticated arbitrary file

9.8 **CVE-2025-66256** Dbbroadcast mozart next 100 firmware

Unauthenticated Arbitrary File Upload (patch_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Unrestricted file upload in patch_conte

10 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. 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.