Daily brief, Thursday, December 18, 2025

Dec 17, 7:00 PM to Dec 18, 7:00 PM ET

Generated Nov 9, 2026, 3:58 AM ET

0	0	0	35	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

35 new critical CVEs, 2 new breaches.

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

35

10.0 **CVE-2025-65037** Microsoft azure container apps

Improper control of generation of code ('code injection') in Azure Container Apps allows an unauthorized attacker to execute code over a network.

9.9 **CVE-2025-64663** Microsoft azure language

Custom Question Answering Elevation of Privilege Vulnerability

9.8 **CVE-2025-60180** Crmperks wp gravity forms salesforce

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Salesforce gf-salesforce-crmperks allows Object Injection.This issue affects WP Gravity Forms Salesforce: from n/a through <= 1.5.1.

9.8 **CVE-2025-14860** Mozilla firefox

Use-after-free in the Disability Access APIs component. This vulnerability was fixed in Firefox 146.0.1.

9.8 **CVE-2025-14879** Tenda wh450 firmware DETECTION

A weakness has been identified in Tenda WH450 1.0.0.18. Affected is an unknown function of the file /goform/onSSIDChange of the component HTTP Request Handler. This manipulation of the argument ssid_index causes stack-based buffer overflow. It is possible to i

9.8 **CVE-2023-53941** Easyphp webserver

EasyPHP Webserver 14.1 contains an OS command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by injecting malicious payloads through the app_service_control parameter. Attackers can send POST requests to /ind

9.4 **CVE-2025-65008**

In WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) due to lack of validation in the langGet parameter in the adm.cgi endpoint, the malicious attacker can execute system shell commands. The vendor was notified early about this vulnerability, but

9.8 **CVE-2025-14878** Tenda wh450 firmware

A security flaw has been discovered in Tenda WH450 1.0.0.18. This impacts an unknown function of the file /goform/wirelessRestart of the component HTTP Request Handler. The manipulation of the argument GO results in stack-based buffer overflow. The attack may

9.8 **CVE-2025-56157** Langgenius dify

Default credentials in Dify thru 1.5.1. PostgreSQL username and password specified in the docker-compose.yaml file included in its source code. NOTE: the Supplier reports that the Docker configuration does not make PostgreSQL (on TCP port 5432) exposed by defa

9.1 **CVE-2025-68398** Weblate weblate

Weblate is a web based localization tool. In versions prior to 5.15.1, it was possible to overwrite Git configuration remotely and override some of its behavior. Version 5.15.1 fixes the issue.

10.0 **CVE-2025-65041** Microsoft partner center

Improper authorization in Microsoft Partner Center allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2025-63389** Ollama ollama

A critical authentication bypass vulnerability exists in Ollama platform's API endpoints in versions prior to and including v0.12.3. The platform exposes multiple API endpoints without requiring authentication, enabling remote attackers to perform unauthorized

9.8 **CVE-2025-53433**

Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes EasyEat easyeat allows PHP Local File Inclusion.This issue affects EasyEat: from n/a through <= 1.9.0.

9.8 **CVE-2025-60089** Crmperks wp gravity forms freshdesk plugin

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms FreshDesk Plugin gf-freshdesk allows Object Injection.This issue affects WP Gravity Forms FreshDesk Plugin: from n/a through <= 1.3.5.

9.8 **CVE-2025-60090** Crmperks wp gravity forms insightly

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Insightly gf-insightly allows Object Injection.This issue affects WP Gravity Forms Insightly: from n/a through <= 1.1.6.

9.8 **CVE-2025-60091** Crmperks wp gravity forms zoho crm and bigin

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Zoho CRM and Bigin gf-zoho allows Object Injection.This issue affects WP Gravity Forms Zoho CRM and Bigin: from n/a through <= 1.2.9.

9.8 **CVE-2025-60174** Crmperks wp gravity forms constant contact plugin

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Constant Contact Plugin gf-constant-contact allows Object Injection.This issue affects WP Gravity Forms Constant Contact Plugin: from n/a through <= 1.1.2.

9.8 **CVE-2025-60178** Crmperks wp gravity forms hubspot

Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms HubSpot gf-hubspot allows Object Injection.This issue affects WP Gravity Forms HubSpot: from n/a through <= 1.2.6.

9.8 **CVE-2025-64206**

Deserialization of Untrusted Data vulnerability in TieLabs Jannah jannah allows Object Injection.This issue affects Jannah: from n/a through <= 7.6.0.

9.8 **CVE-2025-54723**

Deserialization of Untrusted Data vulnerability in BoldThemes DentiCare denticare allows Object Injection.This issue affects DentiCare: from n/a through < 1.4.3.

15 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 2

AUTOSUR autosur.fr	487,226 accounts
The Botting Network thebotnet.com	96,320 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.