

High-Severity CVEs for Ubuntu 22.04.4 LTS \n \l Linux 6.1.123+ x86_64 (as of 2025-08-12 08-26)

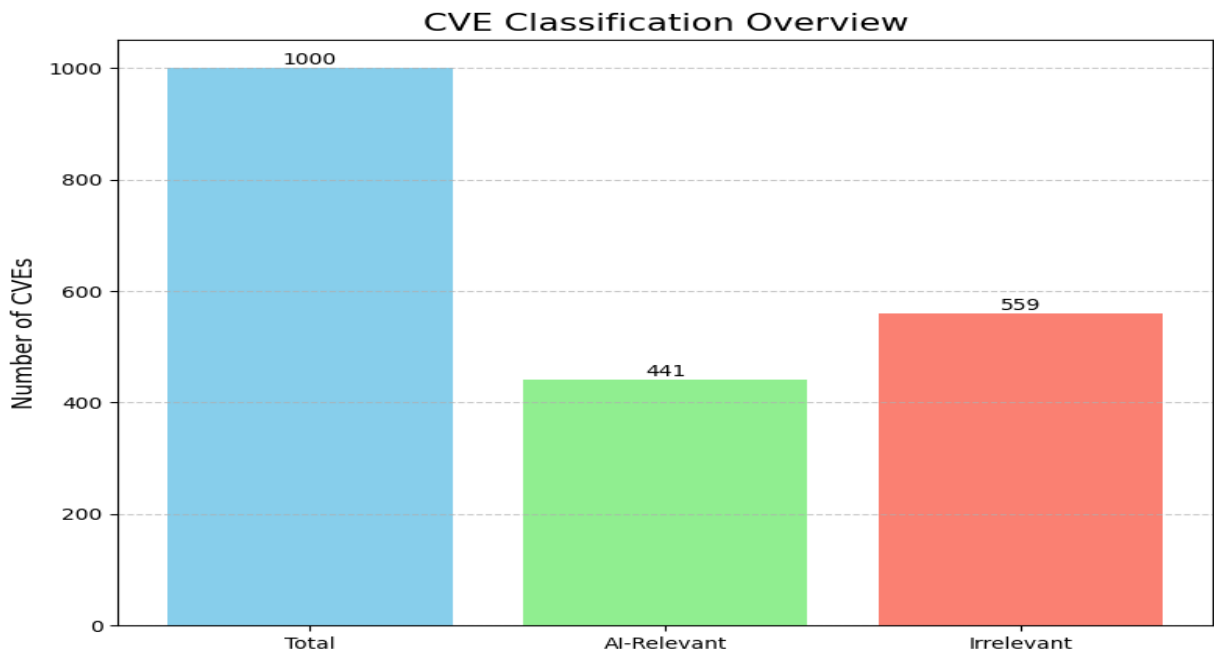
System Info: {'os': 'Linux', 'version': '#1 SMP PREEMPT_DYNAMIC Sun Mar 30 16:01:29 UTC 2025', 'kernel': '6.1.123+', 'arch': 'x86_64'}

CVE Date Range: 2025-01-01 to 2025-08-04

Total AI-Relevant CVEs: 441

Total AI-Irrelevant CVEs: 559

■ CVE Classification Summary



Top AI Keyword Matches:

0.9.10, 3.30.0, 4.0.10, account takeover, acls, addon, aes, android, authentication bypass, bfd_putl64

High-Severity CVE Table:

| S.NuM. | CVE_ID | CVSS_Score | AI Description |
|--------|-------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | CVE-2025-0147 | 9.8 | Zoom Workplace App for Linux before 6.2.10 may allow an authorized user |
| 2 | CVE-2025-0177 | 9.8 | Javo Core plugin for WordPress is vulnerable to privilege escalation in all versions up to 3.0.080 . This is due to the plugin allowing users who are registering new accounts to set their own role . |
| 3 | CVE-2025-0180 | 9.8 | The WP Foodbakery plugin for WordPress is vulnerable to privilege escalation in all versions up to 3.3 . This is due to the plugin not properly restricting what user meta can be updated during |
| 4 | CVE-2025-0181 | 9.8 | The WP Foodbakery plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to 4.7 . This is due to the plugin not properly validating a user's identity prior to setting the current user |
| 5 | CVE-2025-0456 | 9.8 | The airPASS from NetVision Information has a Missing Authentication vulnerability . Remote attackers can access the |
| 6 | CVE-2025-0316 | 9.8 | The WP Directorybox Manager plugin for WordPress is vulnerable to authentication bypass in versions up to 2.5 . This is due to incorrect authentication in the 'WP_DP_enquiry_agent_contact — |

| S.NuM. | CVE_ID | CVSS_Score | AI Description |
|--------|-------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7 | CVE-2025-0357 | 9.8 | The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'WPB_Profile_controller::handle_image_upload' function |
| 8 | CVE-2025-0455 | 9.8 | The airPASS from NetVision Information has a SQL Injection vulnerability . Remote attackers can |
| 9 | CVE-2025-0493 | 9.8 | MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to Limited Local File Inclusion in all versions up to, and including, 4.2.14 via the tabname parameter . This makes it possible for unauthenticated attackers to include PHP files on the server |
| 10 | CVE-2025-0486 | 9.8 | A vulnerability was found in Fanli2012 native-php-cms 1.0.0 . Affected by unknown functionality of the file /fladmin/login.php . Attack can be launched remotely |
| 11 | CVE-2025-0532 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 . Affected is an unknown function of the file /dashboard/admin/new_submit.php . The manipulation of the argument |
| 12 | CVE-2025-0541 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 . This issue affects some unknown processing of the file /dashboard/admin/edit_member.php . The attack may be initiated remotely . |

| S.NuM. | CVE_ID | CVSS_Score | AI Description |
|--------|-------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | CVE-2025-0880 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 and classified as critical . This issue affects some unknown processing of the file /dashboard/admin/upda teplan.php |
| 14 | CVE-2025-0562 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 and classified as critical . This issue affects some unknown processing of the file /dashboard/admin/healt h_status_ |
| 15 | CVE-2025-0585 | 9.8 | The a+HRD from aEnrich Technology has a SQL Injection vulnerability . |
| 16 | CVE-2025-0668 | 9.8 | Vulnerability in BOINC Server allows Stored XSS or 'Cross-site Script |
| 17 | CVE-2025-0767 | 9.8 | WP Activity Log 5.3.2 was found to be vulnerable |
| 18 | CVE-2025-0838 | 9.8 | There exists a heap buffer overflow vulnerable in Abseil-cpp . The sized constructors, reserve() and rehash() methods of absl::{f lat,node}hash{set,map} did not impose an upper bound on their size argument . We recommend upgrading past commit 5a0e |
| 19 | CVE-2025-0842 | 9.8 | A vulnerability was found in needyamin Library Card System 1.0 and classified as critical . This issue affects some unknown processing of the file admin.php of the component Login.php . The attack may be |

| S.NuM. | CVE_ID | CVSS_Score | AI Description |
|--------|-------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20 | CVE-2025-0855 | 9.8 | The PGS Core plugin for WordPress is vulnerable to PHP Object Injection in all versions up to 5.8.0 . This makes it possible for unauthenticated attackers to inject a PHP Object . No known POP chain is present in the vulnerable software . |
| 21 | CVE-2025-1023 | 9.8 | A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries . The newCountName is directly concatenated into an SQL query without proper sanitization . |
| 22 | CVE-2025-0881 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 . Affected is an unknown function of the file /dashboa rd/admin/saveroutine.php . The manipulation of the argument |
| 23 | CVE-2025-0890 | 9.8 | Zyxel VMG4325-B10A firmware version 1.00(AAF R.4)C0_20170615 could allow an attacker to log |
| 24 | CVE-2025-0912 | 9.8 | The Donations Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.19.4 . This makes it possible for unauthenticated attackers to inject a PHP Object |

| S.NuM. | CVE_ID | CVSS_Score | AI Description |
|--------|-------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25 | CVE-2025-1093 | 9.8 | AIHub theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the generate_image function . This makes it possible for unauthenticated attackers to upload arbitrary files |
| 26 | CVE-2025-1061 | 9.8 | The Nextend Social Login Pro plugin for WordPress is vulnerable to authentication bypass . This is due to insufficient verification on the user being supplied during the Apple OAuth authenticate request through the plugin . This makes it possible for unauthenticated attackers to log in as |
| 27 | CVE-2025-1128 | 9.8 | Everest Forms is vulnerable to arbitrary file upload, read, and deletion due to missing file type and path validation in the 'format' method of the EVF_Form_Fields_Upload class in all versions up to, and including, 3.0.9.4.4 . This makes it possible for un |
| 28 | CVE-2025-0108 | 9.1 | An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required . This issue does not affect Cloud NGFW or Prisma Access software . |

■ Sampled AI-Relevant High Severity CVEs for Manual Review

| S.No. | CVE_ID | CVSS_Score | AI Description | Description |
|-------|-------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | CVE-2025-0486 | 9.8 | A vulnerability was found in Fanli2012 native-php-cms 1.0.0 . Affected by unknown functionality of the file /fladmin/login.php . Attack can be launched remotely | A vulnerability was found in Fanli2012 native-php-cms 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /fladmin/login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. |
| 2 | CVE-2025-1061 | 9.8 | The Nextend Social Login Pro plugin for WordPress is vulnerable to authentication bypass . This is due to insufficient verification on the user being supplied during the Apple OAuth authenticate request through the plugin . This makes it possible for unauthenticated attackers to log in as | The Nextend Social Login Pro plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.1.16. This is due to insufficient verification on the user being supplied during the Apple OAuth authenticate request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email. |

| S.No. | CVE_ID | CVSS_Score | AI Description | Description |
|-------|-------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | CVE-2025-0456 | 9.8 | The airPASS from NetVision Information has a Missing Authentication vulnerability . Remote attackers can access the | The airPASS from NetVision Information has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to access the specific administrative functionality to retrieve * all accounts and passwords. |
| 4 | CVE-2025-0881 | 9.8 | A vulnerability was found in Codezips Gym Management System 1.0 . Affected is an unknown function of the file /dashboard/admin/saveroutine.php . The manipulation of the argument | A vulnerability was found in Codezips Gym Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /dashboard/admin/saveroutine.php . The manipulation of the argument rname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. |

| S.No. | CVE_ID | CVSS_Score | AI Description | Description |
|-------|-------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5 | CVE-2025-0108 | 9.1 | An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required . This issue does not affect Cloud NGFW or Prisma Access software . | An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue does not affect Cloud NGFW or Prisma Access software. |

■ CVE Severity Summary

