

Step-by-Step Walkthrough: Showcasing Key Features of vschat 3.2

Detailed guide to software's main functions and
tools

Introduction to the Software and Overview of User Interface

Software Introduction

Introducing the software highlights its primary purpose and key functionalities for users.

User Interface Layout

The layout consists of main sections arranged for easy access and efficient workflow.

Navigation Features

Users can navigate through the platform using menus, buttons, and shortcuts designed for usability.

After clicking on the Search Query tab, enter your natural language query.

In this case the user is searching for vulnerabilities with low attack complexity - a measure of ease of exploitation - that are known to be involved in ransomware attacks.

Once the **Execute Query** button is clicked, the system runs the query and displays the CVE id, vendor, product and date published from the National Vulnerability Database. You can see the total rows found, view the first fifty records here and optionally download all rows up to 1000 total records in a CSV formatted file.

There is a circular selector that is designed to provide transparency and build trust: clicking on **Conf** button produces the Inference Confidence displaying the AI's confidence level that the generated SQL statement correctly reflects what was asked.

Search Query CVE Analysis

Show the CVE id, vendor, product, and date published for cves in which attack complexity is low and are involved in ransomware

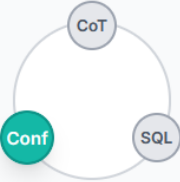
Execute Query Reset (Ctrl+R) History (Ctrl+H)

Status: idle | Conn:connected | Duration: 22s

Inference Confidence

SQL Generation Confidence 100.0%

Very High: The model is very confident about the generated SQL.



Inference Confidence

Total rows: 280 Showing first 50 rows

[Download CSV](#)

id	vendor	product	published
CVE-2025-10035	Fortra	GoAnywhere MFT	2025-09-18
CVE-2025-31161	CrushFTP	CrushFTP	2025-04-03
CVE-2025-31324	SAP	NetWeaver	2025-04-24
CVE-2024-0012	Palo Alto Networks	PAN-OS	2024-11-18
CVE-2024-11667	Zyxel	Multiple Firewalls	2024-11-27

Search Query CVE Analysis

Show the CVE id, vendor, product, and date published for cves in which attack complexity is low and are involved in ransomware

Execute Query

Reset (Ctrl+R)

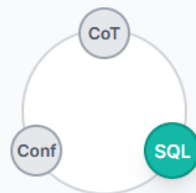
History (Ctrl+H)

Status: idle | Conn:connected | Duration: 22s

Generated SQL

```
SELECT n.id, n.vendorProject AS vendor, n.product, n.published FROM n LIMIT 1000
```

Copy



Generated SQL

Total rows: 280

Showing first 50 rows

Download CSV

id	vendor	product	published
CVE-2025-10035	Fortra	GoAnywhere MFT	2025-09-18
CVE-2025-31161	CrushFTP	CrushFTP	2025-04-03
CVE-2025-31324	SAP	NetWeaver	2025-04-24
CVE-2024-0012	Palo Alto Networks	PAN-OS	2024-11-18

You can click on the **SQL** button to see the actual SQL statement that the LLM generated from your original question. Optionally, you can copy this statement to your clip board

[Search Query](#)

CVE Analysis

Show the CVE id, vendor, product, and date published for cves in which attack complexity is low and are involved in ransomware

Execute Query

Reset (Ctrl+R)

History (Ctrl+H)

Status: idle | Conn: connected | Duration: 22s

Chain of Thought Reasoning

1. Identify the tables and fields needed:

- From `non_cvss_data`: `id`, `vendorProject`, `product`, `published`, `knownRansomwareCampaignUse`
- From `cvssMetricV31`: `id`, `metrics_cvssMetricV31_cvssData_attackComplexity`

2. Construct the JOIN condition:

- Join `non_cvss_data` and `cvssMetricV31` on the `id` field.

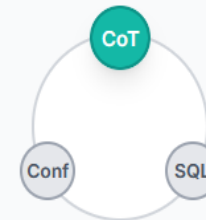
3. Apply filters:

- For attack complexity: `LOWER(metrics_cvssMetricV31_cvssData_attackComplexity) = 'low'` (STRING field, use LOWER())
- For ransomware involvement: `LOWER(knownRansomwareCampaignUse) = 'known'` (STRING field, use LOWER())

4. Select the required fields:

- `id`, `vendorProject`, `product`, `published`

5. Construct the SQL query using the above conditions and selections.



Chain-of-Thought

The **CoT** button presents the Chain of Thought Reasoning that the AI used to construct the SQL statement.

Search Query CVE Analysis

Show the CVE id, vendor, product

Execute Query

Reset (Ctrl+)

Status: idle | Conn:connected | Durat

Inference Confidence

SQL Generation Confidence

Very High: The model is very c

Total rows: 280

Query History

Clear All X

Query #10

11/5/2025, 12:29:15 PM

Show the CVE id, vendor, product, and date published for cves in which attack complexity is low and are involved in ransomware

Delete

Query #9

11/4/2025, 11:44:35 AM

Find all CVEs in which requiredAction contains 'apply mitigations' that were published in 2024. Limit 20.

Delete

Query #8

11/4/2025, 11:38:50 AM

Find products with at least 2 vulnerabilities in the top EPSS percentile per year since 2021

Delete

Click on any query to use it again. Showing last 10 of 10 queries.

Use Ctrl+H to quickly access this history, Esc to close

Showing first 50 rows

Download CSV

id	vendor	product	published
CVE-2025-10035	Fortra	GoAnywhere MFT	2025-09-18
CVE-2025-31161	CrushFTP	CrushFTP	2025-04-03
CVE-2025-31324	SAP	NetWeaver	2025-04-24
CVE-2024-0012	Palo Alto Networks	PAN-OS	2024-11-18

Selecting the **History** button shows the last ten queries you used. Clicking on any query in this box will automatically fill the Search Query box with that saved query.

Let's assume you copied the CSV file by clicking on the Download CSV button and have opened it.

The downloaded CSV file is viewable in Excel and contains all 280 records. Let's drill down on a particular threat.

Notice the id CVE-2024-0012 for Palo Alto Networks PAN-OS in row 5. Assume that you have the product in your environment and want to know more about this threat and how to patch it.

To do this, you highlighted and copy "CVE-2024-0012" in column A, row 6 to your clipboard.

	A	B	C	D
1	id	vendor	product	published
2	CVE-2025-10035	Fortra	GoAnywhere MFT	9/18/2025
3	CVE-2025-31161	CrushFTP	CrushFTP	4/3/2025
4	CVE-2025-31324	SAP	NetWeaver	4/24/2025
5	CVE-2024-0012	Palo Alto Networks	PAN-OS	11/18/2024
6	CVE-2024-11667	Zyxel	Multiple Firewalls	11/27/2024
7	CVE-2024-55956	Cleo	Multiple Products	12/13/2024
8	CVE-2024-55591	Fortinet	FortiOS and FortiProxy	1/14/2025
9	CVE-2025-23006	SonicWall	SMA1000 Appliances	1/23/2025
10	CVE-2024-40766	SonicWall	SonicOS	8/23/2024
11	CVE-2024-6670	Progress	WhatsUp Gold	8/29/2024
12	CVE-2024-40711	Veeam	Backup & Replication	9/7/2024
13	CVE-2024-41713	Mitel	MiCollab	10/21/2024
14	CVE-2024-50623	Cleo	Multiple Products	10/28/2024
15	CVE-2024-51378	CyberPersons	CyberPanel	10/29/2024
16	CVE-2024-3400	Palo Alto Networks	PAN-OS	4/12/2024
17	CVE-2024-4577	PHP Group	PHP	6/9/2024
18	CVE-2024-21887	Ivanti	Connect Secure and Policy S	1/12/2024
19	CVE-2023-22527	Atlassian	Confluence Data Center and	1/16/2024
20	CVE-2024-23897	Jenkins	Jenkins Command Line Inte	1/24/2024
21	CVE-2024-21762	Fortinet	FortiOS	2/9/2024
22	CVE-2024-1709	ConnectWise	ScreenConnect	2/21/2024
23	CVE-2024-27198	JetBrains	TeamCity	3/4/2024
24	CVE-2023-48788	Fortinet	FortiClient EMS	3/12/2024
25	CVE-2023-35078	Ivanti	Endpoint Manager Mobile (f	7/25/2023

Next, you've clicked on **CVE Analysis** and pasted the id "CVE-2024-0012" into the search field and hit the **Summarize** button.

The AI gathers data on the vulnerability from the vschat dataset and summarizes it. If there is an available Provider Urgency rank, it will display that as well.

All data used by the system is updated daily and consists of 10 years of vulnerability data including CVEs added yesterday, merged from the National Vulnerability Database (NVD), the current Known Exploited Vulnerabilities Catalog from the Cybersecurity and Infrastructure Security Agency (CISA), the Exploit Prediction Score (EPSS) from First.org, and Morningside Software's proprietary exploitation probability score.

Search Query **CVE Analysis**

Summarize Remediation Reset (Ctrl+R)

Status: idle | Conn: connected | Duration: 13s

CVE Summary
CVE-2024-0012 Summary

****Vulnerability:**** Authentication bypass in Palo Alto Networks PAN-OS management web interface
****Published:**** November 18, 2024
****Severity:**** Critical (CVSS 9.3)
****Exploitation Status:**** Actively exploited with known ransomware campaign use

Technical Details

- ****Attack Vector:**** Network-based, requiring no authentication or user interaction
- ****Weakness Type:**** CWE-306 (Missing Authentication for Critical Function)
- ****Impact:**** Complete compromise - attackers gain full PAN-OS administrator privileges
- ****Affected Versions:**** PAN-OS 10.2, 11.0, 11.1, and 11.2

Impact

Unauthenticated remote attackers can:

- Gain full administrative access to PAN-OS systems
- Tamper with firewall configurations
- Chain with other vulnerabilities (e.g., CVE-2024-9474) for further privilege escalation
- Potentially deploy ransomware (confirmed campaign usage)

Context

This is an extremely high-risk vulnerability with a 98% estimated exploitation probability. While the risk can be reduced by restricting management interface access to trusted internal IPs, the vulnerability has already been weaponized in ransomware campaigns. Cloud NGFW and Prisma Access are not affected. Organizations should treat this as an emergency patch priority given the critical nature and active exploitation.

Provider Urgency: RED

(continued from previous slide)

All the Common Vulnerability Scoring Systems (CVSS) metrics are present in the data including the latest from CVSS v4.0 such as:

- Attack Complexity
- Privileges Required
- User Interaction
- Confidentiality, Integrity, Availability Impact
- Automatable
- Value Density
- Provider Urgency

Search Query [CVE Analysis](#)

CVE-2024-0012

Summarize Remediation Reset (Ctrl+R)

Status: idle | Conn: **connected** | Duration: 13s

CVE Summary
CVE-2024-0012 Summary

****Vulnerability:**** Authentication bypass in Palo Alto Networks PAN-OS management web interface
****Published:**** November 18, 2024
****Severity:**** Critical (CVSS 9.3)
****Exploitation Status:**** Actively exploited with known ransomware campaign use

Technical Details

- ****Attack Vector:**** Network-based, requiring no authentication or user interaction
- ****Weakness Type:**** CWE-306 (Missing Authentication for Critical Function)
- ****Impact:**** Complete compromise - attackers gain full PAN-OS administrator privileges
- ****Affected Versions:**** PAN-OS 10.2, 11.0, 11.1, and 11.2

Impact

Unauthenticated remote attackers can:

- Gain full administrative access to PAN-OS systems
- Tamper with firewall configurations
- Chain with other vulnerabilities (e.g., CVE-2024-9474) for further privilege escalation
- Potentially deploy ransomware (confirmed campaign usage)

Context

This is an extremely high-risk vulnerability with a 98% estimated exploitation probability. While the risk can be reduced by restricting management interface access to trusted internal IPs, the vulnerability has already been weaponized in ransomware campaigns. Cloud NGFW and Prisma Access are not affected. Organizations should treat this as an emergency patch priority given the critical nature and active exploitation.

Provider Urgency: RED

When you click on CVE Analysis | **Remediation**, you will see the remediation steps collected from the vendor's site along with the URL reference.

If remediation steps are not published, you will see a message explaining this and, in all cases, you can follow the reference URL to obtain the latest recommended actions.

Search Query

CVE Analysis

CVE-2024-0012

Summarize

Remediation

Reset (Ctrl+R)

Status: idle | Conn: **connected** | Duration: 12s

Remediation Steps

Based on the CVE-2024-0012 advisory content, here are the clear remediation steps:

Primary Remediation Steps

1. **Restrict Management Interface Access** - Secure access to your management interface by restricting access to only trusted internal IP addresses to prevent external access from the internet, following Palo Alto Networks best practice deployment guidelines.

Additional Protection Steps (If Threat Prevention Subscription Available)

2. **Configure Threat Prevention Blocking** - Set all the following Threat IDs to block mode: 95746, 95747, 95752, 95753, 95759, and 95763 (available in Applications and Threats content version 8915-9075 and later).

3. **Route Management Traffic** - Route incoming traffic for the MGT port through a DP port by enabling management profile on a DP interface for management access.

4. **Replace Management Certificate** - Replace the Certificate for Inbound Traffic Management.

5. **Enable Traffic Decryption** - Decrypt inbound traffic to the management interface so the firewall can inspect it.

6. **Enable Threat Prevention** - Enable threat prevention on the inbound traffic to management services.

Important Notes

- This vulnerability affects PAN-OS versions 10.2, 11.0, 11.1, and 11.2 on PA-Series, VM-Series, CN-Series firewalls, and Panorama
- Cloud NGFW and Prisma Access are not impacted
- The primary mitigation (restricting management interface access) is the most critical step

Reference:

Reference: <https://security.paloaltonetworks.com/CVE-2024-0012>

Conclusion

Software Overview

The walkthrough covered essential software aspects, including the user interface and key functionalities.

Advanced Features

Advanced features were explored to enhance the user's ability to use the software effectively.

Workflow Optimization

Understanding the software helps maximize its potential for improving workflows and productivity.