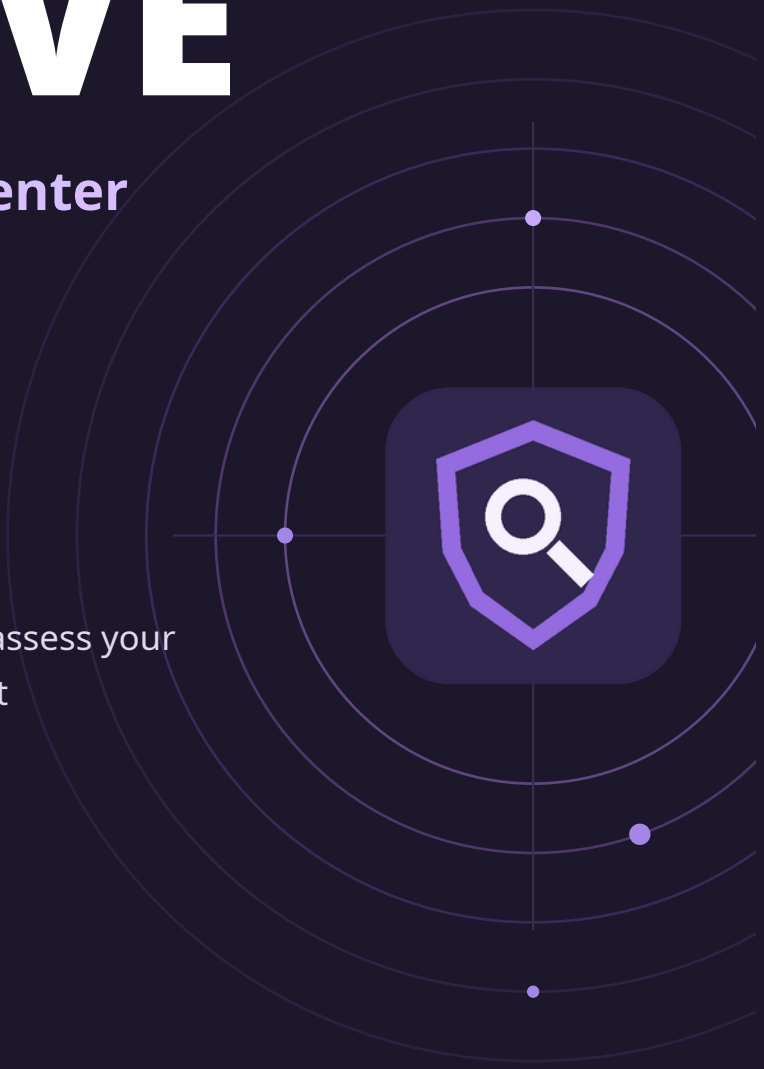
VERSION 2.0.5

WinCVE

Explorer & Control Center



User Manual

Explore the vulnerability catalog, assess your Windows computer and document remediation.

Windows desktop interface and command line

x64, x86 and ARM64 editions

Oscar de la Cuesta Campillo

WinCVE project · palentino.es

27 November 2026

READING GUIDE

Contents

Select a chapter below or use the PDF bookmarks. The Contents link in each page header brings you back here.

Download, install and start 03
Architectures, formats and SHA-256

Home and navigation 04
Dashboard, quick actions and shortcuts

Local catalog and data sources 05
Synchronization and offline lookup

Update and verify data sources 06
NVD, KEV, EPSS and verification

Explore and filter CVEs 07
Filters, record details and page CSV

Search by UTC date 08
Publication and import examples

Read indicators and prioritize 09
CVSS, KEV, EPSS and priorities P1-P5

Inventory and correlation 10
Evidence, coverage and the CPE dictionary

From findings to a decision 11
Versions, affected ranges and advisories

Windows, patches and audit 12
Build, KB updates and MSRC releases

Network and firmware 13
Local inventory and device profiles

Reports and history 14
Report Studio PRO and export formats

Read a unified assessment 15
Coverage, statuses and actions

Configure an AI provider 16
OpenAI, OpenRouter, models and keys

Review a CVE with AI 17
Walkthrough with CVE-2024-11477

Local AI with Ollama and LM Studio 18
Prepare a model and test the connection

AI from PowerShell 19
Models, environment variables and topics

Troubleshoot AI 20
HTTP errors, models and saved profiles

Personalization and integrations 21
Languages, themes and Palentino tools

Get started with the command line 22
Help, diagnostics and lookup by ID

Repeatable queries and tasks 23
PowerShell, JSON and exit codes

CLI quick reference 24
Commands by task and built-in help

Back up, restore and migrate 25
Local data and portable catalogs

Two end-to-end walkthroughs 26
Apply an advisory and move a catalog

Troubleshooting 27
Symptoms, checks and recovery

Sources and credits 28
Downloads, support and documentation

Your first session

Import the bundled catalog and look up a known CVE. The screenshots show the Spanish interface. Where a control still appears in Spanish in this release, the guide gives its on-screen wording.

Configure an AI provider ›

Review a CVE step by step ›

01 / INSTALLATION

Download, install and start

Palentino publishes six self-contained WinCVE 2.0.5 packages with the catalog included. There is one package for each architecture and format. The .NET runtime is bundled.

Your computer	Edition	Available formats
64-bit Windows on Intel or AMD	**x64**	EXE installer and portable ZIP
Compatible 32-bit Windows	**x86**	EXE installer and portable ZIP
Windows on a 64-bit ARM processor	**ARM64**	EXE installer and portable ZIP

1. **Check your system type.** In Windows, open **Settings › System › About**. Check the architecture under **System type** and select the matching download on Palentino.
2. **Verify the download.** Run the example below in PowerShell from your Downloads folder. Replace the filename with yours and compare all 64 characters with the published SHA-256 hash for that exact file.

```powershell
$file = ".\WinCVE-2.0.5-win-x64-con-catalogo-setup.exe"
Get-FileHash -Algorithm SHA256 -Path $file
```

3. **Install or extract.** For the EXE, follow the setup wizard and open WinCVE from its shortcut. For the ZIP, extract all files to a writable folder and run **WinCVE.exe** there.
4. **Load the bundled catalog.** If the database is empty, WinCVE offers to import **WinCVE-Catalogo.zip** offline. When it finishes, check the record count in **Updates**. You can also run **IMPORTAR_CATALOGO_INCLUIDO.bat** with WinCVE closed.

> **Allow space for the import**
>
> Leave room for the extracted files and the SQLite database created during import. Download the prebuilt packages from the project website.

Find the downloads and published hashes ›

02 / DASHBOARD

Home and navigation

The dashboard brings together computer findings, data source status and scan history. Counts reflect the current session and the catalog loaded on your computer.

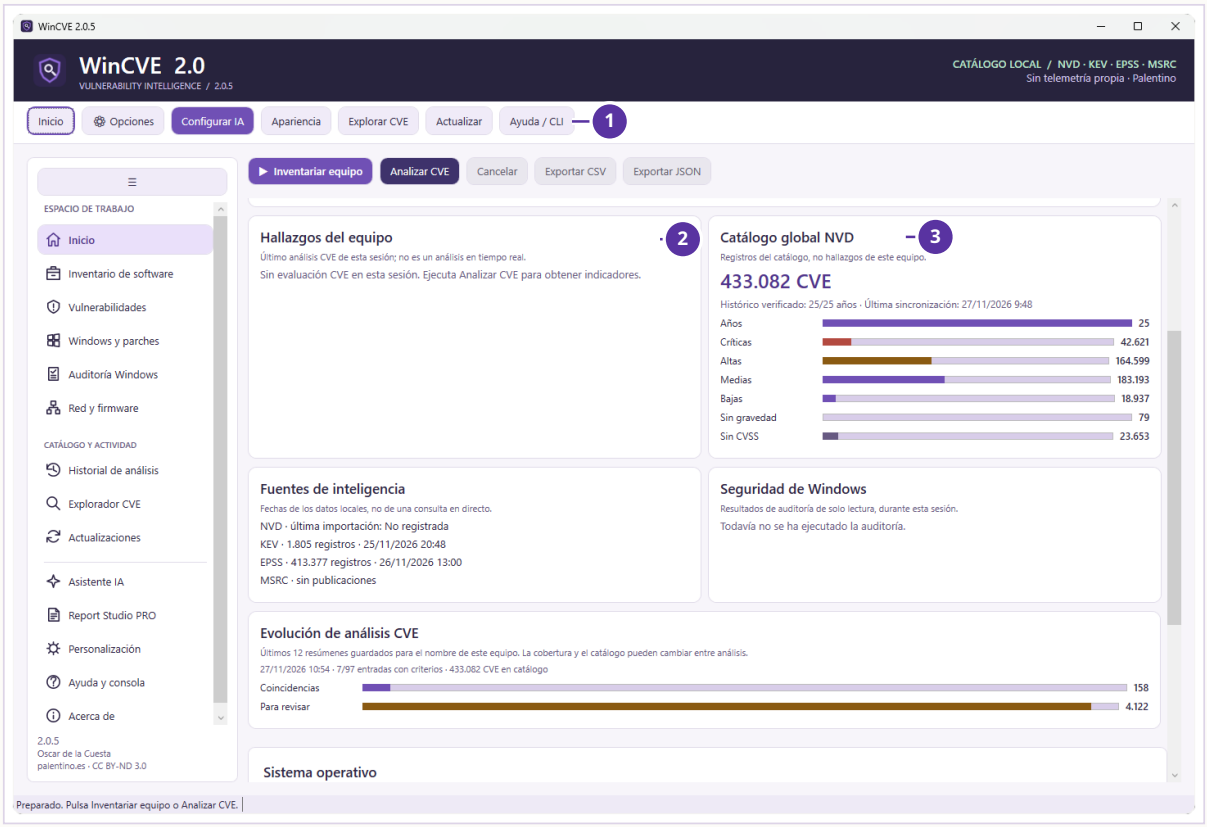


Figure 1. The WinCVE 2.0.5 Home page. Palentino published this screenshot on 27 November 2026.

1 **Top toolbar.** Use **Opciones** (Options), **Configurar IA** (Configure AI), **Explorar CVE** (Explore CVEs), **Actualizar** (Updates) and **Ayuda / CLI** (Help / CLI).

2 **Computer findings.** Run **Scan CVEs** to populate this panel. The trend view displays up to 12 saved summaries for this computer.

3 **Global NVD catalog.** Check the record count and coverage of the local copy. The panel below shows dates for KEV, EPSS and MSRC.

Keyboard shortcuts

Open	Shortcut	Open	Shortcut
CVE explorer	Ctrl+F	Updates	Ctrl+U
Configure AI	Ctrl+I	Scan history	Ctrl+H
Options	Ctrl+,	Help and command center	F1 or Ctrl+T

03 / LOCAL DATA

Local catalog and data sources

WinCVE stores records in SQLite. Use the local copy offline and connect when you need to refresh it.

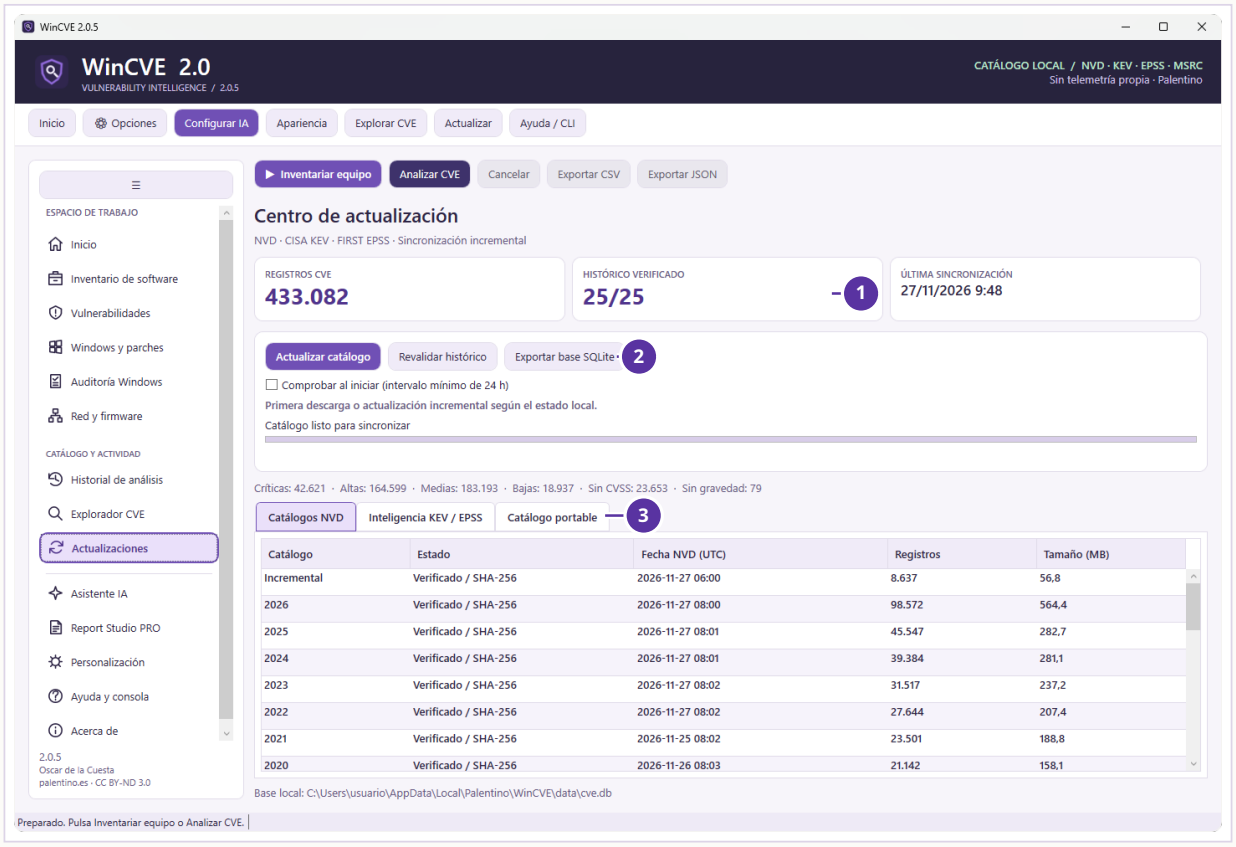


Figure 2. The update center shows catalog coverage and the date of the last successful sync.

1. **Check coverage.** In **Updates**, review the record count, verified history and last sync. Check the status and UTC date of each feed in the table.
2. **Update NVD.** Select **Update catalog** for a routine update. Use **Revalidate history** to check the annual feeds when you need to confirm coverage.
3. **Refresh the intelligence feeds.** Open **KEV / EPSS intelligence** and select **Update KEV and EPSS**. Use **Portable catalog** to verify, export or restore a catalog.

MSRC and the CPE dictionary

The Windows & patches module synchronizes its own MSRC releases. The CPE dictionary can be imported locally from official NIST files.

Check at startup checks the catalog when WinCVE opens, with at least 24 hours between checks.

04 / UPDATES

Update and verify data sources

The dashboard reads local copies with their own dates. Before assessing a computer, check historical coverage and the date of the data you will rely on.

How WinCVE chooses an NVD update mode

Situation	What version 2.0.5 does
Complete and recent catalog	Checks the NVD modified feed. When new content is downloaded, WinCVE verifies the date, size and SHA-256 hash.
Missing years or a copy outside the update window	Checks historical feeds from 2002 onward. WinCVE uses a seven-day cutoff to decide when it needs to recover the history.
Revalidate history	Checks the annual and modified feed metadata. If the hash matches, WinCVE can update the feed timestamp without downloading the same content again.

Update each source in its own view

1. **NVD.** Go to **Updates › Update catalog** for a routine update. For a local file, use **CVE explorer › Import NVD JSON / GZ** and check the import result.
2. **CISA KEV and FIRST EPSS.** In **Updates › KEV / EPSS intelligence**, select **Update KEV and EPSS**. **Import KEV / EPSS offline** accepts CISA JSON and GZIP-compressed FIRST CSV files.
3. **Windows and patches.** Select **Sync MSRC** and check which months are available under **Local releases**.

> **Check the result of an interrupted sync**
>
> WinCVE keeps feeds whose imports already completed. Check each feed status and the last completed sync. If the update reports future-dated metadata, check the Windows date and time before retrying.

NIST · NVD data feeds and metadata ›

05 / CATALOG LOOKUP

Explore and filter CVEs

In **CVE explorer**, search by the full identifier or by keywords from the description. Use severity and CVE year to narrow a broad search.

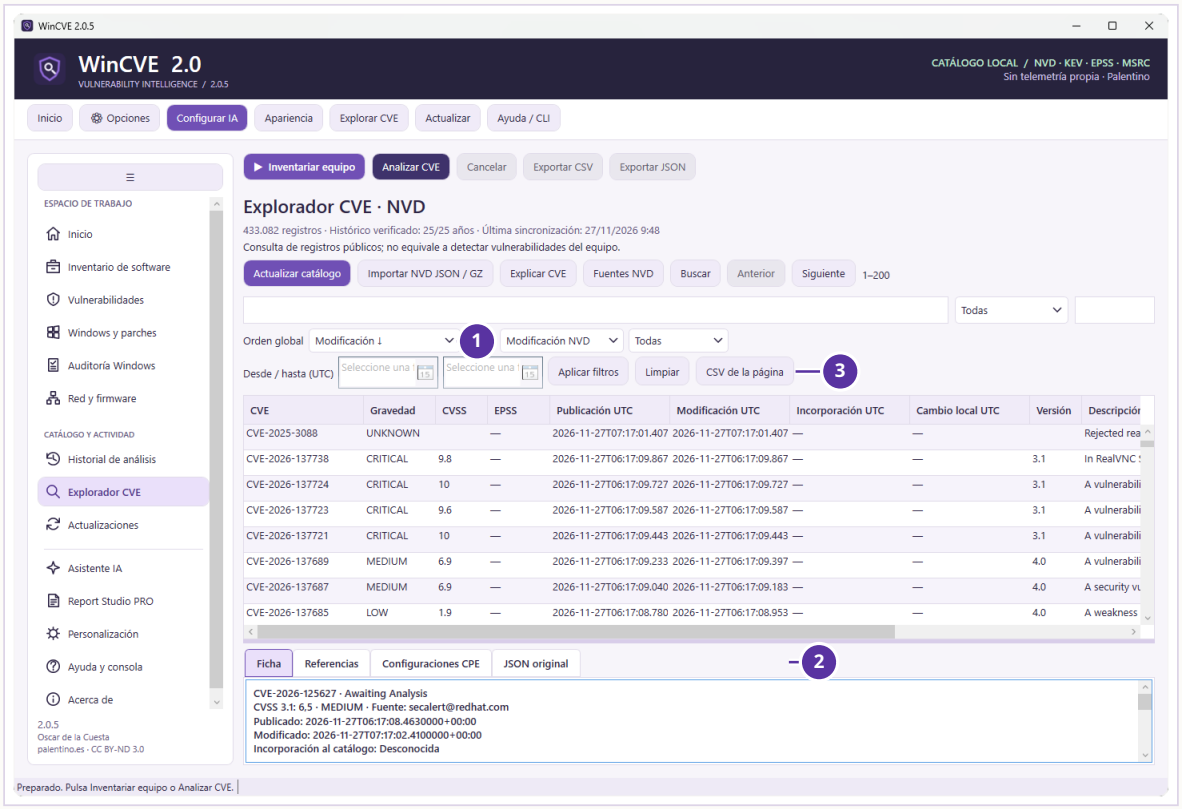


Figure 3. CVE explorer with global sorting, UTC date filters and four detail tabs.

1. **Sort and filter.** Choose **Orden global** (global sort), **Fecha** (date field) and a period. Select **Aplicar filtros**. Sort the full result set by date, CVSS, EPSS or severity.
2. **Read the details.** Select a row and open **Details**, **References**, **CPE configurations** or **Raw JSON**.
3. **Export the visible page. CSV de la página** saves the visible rows with dates and descriptions. Use **Previous** and **Next** to browse further.

UTC field	What it records
NVD publication	The date the source first published the record.
NVD modification	The latest change date reported by NVD.
First import	The first import of this CVE recorded by your local copy.
Last local change	The last actual change imported. **Desde última sinc.** uses this field.

06 / FILTERS AND SORTING

Search by UTC date

In the explorer, **Fecha** selects the date field to filter and **Orden global** sets the sort order. You can set them independently.

Question	Explorer settings	Result
What was published this week?	Choose **Publicación NVD** (NVD publication) and **Últimos 7 días** (last 7 days). Sort by **Publicación** descending.	Records first published during the selected period.
What was revised this month?	Choose **Modificación NVD**, then **Personalizado** (custom) and enter the UTC dates. Sort by **Modificación** descending.	Records with an NVD-reported change in that interval.
What was added to my catalog?	Choose **Primera importación** (first import) and a period. Sort by **Incorporación** descending.	Records with a documented first import in your local copy.

One record can have four dates

In this example, NVD publishes a CVE on 18 November and revises it on the 26th. WinCVE first imports it on the 24th and downloads the revision on the 27th.

Field	Example date	Where the date comes from
NVD publication	18 November	First publication by the source.
NVD modification	26 November	Latest revision published by NVD.
First import	24 November	First import recorded in this copy.
Last local change	27 November	Import of the revised record.

Two details when reviewing results

The year filter uses the four digits in the CVE identifier. **Desde última sinc.** (since last sync) uses the last local change and starts at the timestamp of the last completed sync. Local date filters exclude unknown local dates.

07 / VULNERABILITY INTELLIGENCE

Read indicators and prioritize

Start with the product and version. Once you have checked whether the advisory applies, use the catalog indicators to decide what to remediate first.

Indicator	How to use it
CVE and CPE	CVE identifies the vulnerability. CPE identifies the product or platform. Check the vendor, version and applicability criteria.
CVSS	Technical severity on a scale of 0 to 10. Check the scoring standard version and the source of the score when available.
KEV	A CISA listing indicates evidence of exploitation in the wild. Check the published action and the date of your copy.
EPSS	The estimated probability of observing exploitation of a CVE in the next 30 days. Check the score and scoring date.

Priorities in WinCVE 2.0.5

For software and firmware findings, WinCVE assigns the first matching priority in the table below. A blank indicator means that value is missing from the record or the local source.

Priority	WinCVE criterion
P1 · KEV	The CVE appears in the available KEV catalog.
P2 · EPSS	EPSS of 10% or higher.
P3 · Critical CVSS	CVSS of 9.0 or higher.
P4 · High CVSS	CVSS of 7.0 or higher.
P5 · Assess	Other cases, including those with incomplete indicators.

> **Use evidence from the computer**
>
> For a P1 finding, check the exact installed version and the vendor advisory. Set the remediation deadline based on exposure, operational impact and mitigations already in place.

The EPSS percentile is a relative ranking. WinCVE uses the EPSS probability to determine P2.

Find the CVSS, KEV and EPSS sources ›

08 / LOCAL SOFTWARE

Inventory and correlation

The inventory reads uninstall entries registered for the computer and the current user. Correlation checks mapped products against the local catalog.

1. **Select Inventory computer.** Open **Software inventory**. Filter by name, publisher, version or scope. Select a row to see the registry evidence.
2. **Select Scan CVEs.** Open **Vulnerabilities › Findings**. Check the matched product and version, the CVE identifier and the evidence for that match.
3. **Check coverage.** In **Coverage & unmapped products**, look for entries with missing versions, missing or ambiguous mappings, or no available criteria. Use a separate inventory for portable software, MSIX packages and dependencies.

Common status	What to check
CPE match (Coincidencia CPE)	Verify the vendor, version, edition and affected range in the advisory. Check for patches or product variants that may change applicability.
Review required (Revisión necesaria)	Read the evidence and resolve the outstanding condition. It may depend on version comparison, other components or a complex CPE configuration.
Missing mapping or version	Verify the installed application against the vendor inventory. Add a verified CPE mapping where appropriate and scan again.

Create a verified CPE mapping

In **Vulnerabilities › CPE dictionary**, import the official dictionary as JSON or XML. Select the product in the Coverage tab and choose **Use application from coverage**. Verify the vendor and product before selecting **Save verified mapping**. Run the scan again to use the saved mapping.

> **Close the review with a record**
>
> Record the CVE, installed version, advisory link and decision. If evidence is incomplete, record what is missing and who can verify it.

09 / VALIDATING FINDINGS

From findings to a decision

Start in **Vulnerabilities › Findings**, then use the CVE explorer to check the match. Record what you verified on the computer and the criterion that supports your conclusion.

1. **Identify what WinCVE found.** Note the application, publisher and version shown in the inventory. Open the finding and read the CPE criterion, the affected range and the reason for the match or review.
2. **Open the CVE record.** Search by identifier in **CVE explorer**. Review **CPE configurations** and **References**. Check the original advisory for the product, edition and fixed version.
3. **Check what applies.** Look for optional components, versions from other publishers and fixes backported by your distributor. If the version formats differ, verify the installed version with your inventory tool or the vendor.
4. **Record a decision.** Note what is installed, the date you checked it and why the advisory applies, can be ruled out or needs more evidence. Keep the reference that supports your decision.

How to read a version boundary

Evidence field	Example interpretation
versionEndExcluding = 24.07	This example range ends before 24.07. Version 24.06 falls below that upper bound.
versionEndIncluding = 24.07	This example range includes 24.07. Check the lower bound and other conditions as well.
Review required	Find the condition still to verify, such as a version that cannot be compared or a combination of products.

> **Prioritize remediation**
>
> Use the P1-P5 priority alongside actual software use, exposure and service impact. After remediation, rerun the inventory and record the final version.

10 / OPERATING SYSTEM

Windows, patches and audit

Use WinCVE to review the Windows build and detected KB updates, and to check the state of security controls on the computer.

Assess Windows with MSRC

1. **Select Windows & patches › Inventory Windows / KB.** Note the edition, architecture and build. Check for a pending restart.
2. **Load the releases.** Use **Sync MSRC** online or **Import CVRF JSON** with a trusted local file. Check which months are available under **Local releases**.
3. **Choose the exact MSRC product.** Match the computer edition, version and architecture. Select **Assess build** and open **MSRC assessment** to review each item's evidence and link.

> **If a KB is missing**
>
> Check the current build, the fixed build in Microsoft's advisory and any cumulative updates that supersede the KB. Mark the item as pending verification when evidence is incomplete.

Check controls with Windows audit

Select **Audit Windows** to read the current configuration. The module checks Firewall, Defender, BitLocker, Secure Boot, TPM, UAC, SMB and Remote Desktop, among other controls. Each row shows the status, evidence and data source.

Observation	Follow-up
Check completed	Compare the setting with the policy that applies to the computer.
Check incomplete	Read the reason in the evidence and verify the control with the relevant administration tool.

Export CSV or JSON to attach the results to a report or ticket. The audit is read-only.

11 / DEVICES

Network and firmware

The network inventory shows what the Windows computer has observed. Firmware assessment uses saved device profiles with details you can verify.

Review the local network passively

1. **Open Network & firmware › Network inventory.** Select **Read local network** to see interfaces, gateways and neighbors in the Windows cache.
2. **Verify the observation.** Use the asset inventory or the device management console to identify the device behind each entry. The cache only covers neighbors seen by this Windows computer and may be incomplete.

Assess a known firmware version

1. **Identify the device precisely.** Check the label or management console for a device you manage. Record the vendor, model, hardware revision and firmware version.
2. **Fill out Devices & firmware.** Choose the CPE type (operating system or hardware) and enter the verified vendor and product identifiers alongside the profile details. Select **Save profile**.
3. **Review the CVE assessment.** Select the profile and choose **Assess CVEs**. Compare matches with the vendor advisory for that hardware revision and firmware version. Export CSV or JSON if needed.

Detail	Where to verify it
Model and revision	Device label, management console or asset inventory.
Firmware version	Device status page and version documentation.
Available fix	Vendor security advisory and release notes.

> **Evidence to keep in a firmware report**
>
> Record the model and revision, observed version, date, advisory and the update or review decision.

12 / DOCUMENTATION

Reports and history

Choose the report for the work you performed. Keep the date, scope, evidence and catalog version with the output.

Software report in Report Studio PRO

1. **Run Scan CVEs.** Open **Report Studio PRO** and check that the summary is for the software scan you want to document.
2. **Configure the report.** Enter the title and organization. Choose whether to include the technical appendix and review **Hide computer name, registry paths and warning details**.
3. **Select Generate HTML report.** Save and open the report. For a PDF copy, open the browser print dialog and choose **Save as PDF**.

Unified assessment

Go to **Home › Análisis integral** or **Report Studio PRO**. The assessment covers software, Windows, firmware profiles, the Windows audit and passive network inventory. Select the exact product for MSRC, or choose **Omitir MSRC** (skip MSRC) until you can verify it.

Select **Iniciar análisis integral** (start unified assessment), review each stage's status and export HTML or JSON before closing. The report shows coverage and proposed actions by module.

Format	When to use it
HTML	A readable report or audit record. Open it locally and review the appendix.
CSV	Review inventory, findings or supporting module results in a spreadsheet.
JSON	Keep structured evidence or use the results in another process.

> **History and report sharing**
>
> Use **Scan history** to reopen saved inventories. Export the reports you want to keep and check what versions, evidence and computer details they contain before sharing.

13 / REPORT STUDIO PRO

Read a unified assessment

From **Home › Análisis integral** (unified assessment), check each module's status before reviewing the actions. The report records the coverage for that run.

Status shown	How to read it
Completado (completed)	The module finished within its scope. Review the counts and keep the dates of its data sources.
Parcial (partial)	Some results are available. Review the details for missing checks. MSRC and firmware show this status when assessed because their coverage is limited.
No comprobado (not checked)	A prerequisite is missing, such as a selected MSRC product, the NVD catalog or a firmware profile.
Error	Open the affected module to see the message. Resolve the issue and rerun the assessment you need.

1. **Before you run it.** Refresh the relevant sources, check firmware profiles and select **Cargar productos MSRC** to load the MSRC product list if you can identify the exact Windows product.
2. **In the action list.** Use priorities for software and firmware findings. For each MSRC result, check the build and cumulative update. For Windows audit results, check each setting against the computer's policy.
3. **In the exported file.** The HTML report shows the scope, the first 50 actions and an appendix with all findings. Export JSON to process all rows in another program.

> **Read the counts by module**
>
> If you see two software matches, one MSRC item and three controls to review, record those counts by module. Check each criterion and its evidence before confirming a case.

The unified report may include sensitive product names, versions and evidence. Review the appendix before sharing it.

14 / AI ASSISTANT

Configure an AI provider

Select **Configurar IA** (Configure AI) in the top toolbar, or press **Ctrl+I**. You can set up and test a provider before selecting a CVE.

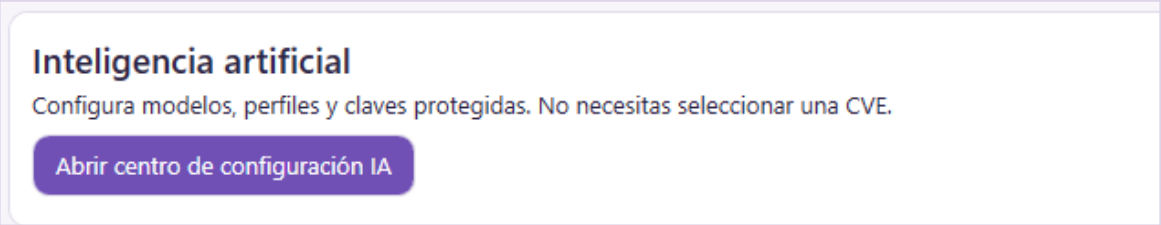


Figure 4. Open the AI Configuration Center from Personalization or the top toolbar.

Set up OpenAI

1. **Get an API key.** On the OpenAI API platform, create a key for a project with API access. The API has its own billing settings, separate from your ChatGPT subscription.
2. **Enter it in WinCVE.** Under **Proveedor** (Provider), select **OpenAI**. Paste the key into **Clave API** (API key). Keep the key out of screenshots, reports and repositories.
3. **Choose a model.** Select **Cargar modelos** (Load models) and authorize the connection. Choose a model that supports chat or paste its full ID into **Modelo (ID exacto)**.
4. **Test the connection.** Select **Probar IA** (Test AI) and authorize the sample request. Check that a reply and a response time in milliseconds appear. The provider may charge for the test.
5. **Save your selection. Guardar perfil** saves the provider profile. **Guardar y usar por defecto** also makes it the assistant's default. Select **Recordar clave cifrada en este equipo** to keep the encrypted key for your Windows account.

If you save the profile without remembering the key, enter it again in the assistant when needed in a later session.

> **Use OpenRouter**
>
> Follow the same steps with an OpenRouter API key and a model ID from its catalog. The provider running the selected model may receive the request.

OpenAI · Where to get an API key ›

OpenRouter · Official quickstart ›

Continue to the CVE walkthrough ›

15 / GUIDED WALKTHROUGH

Review a CVE with AI

Look up **CVE-2024-11477**, a 7-Zip vulnerability, and use the assistant to review applicability, affected versions and remediation.

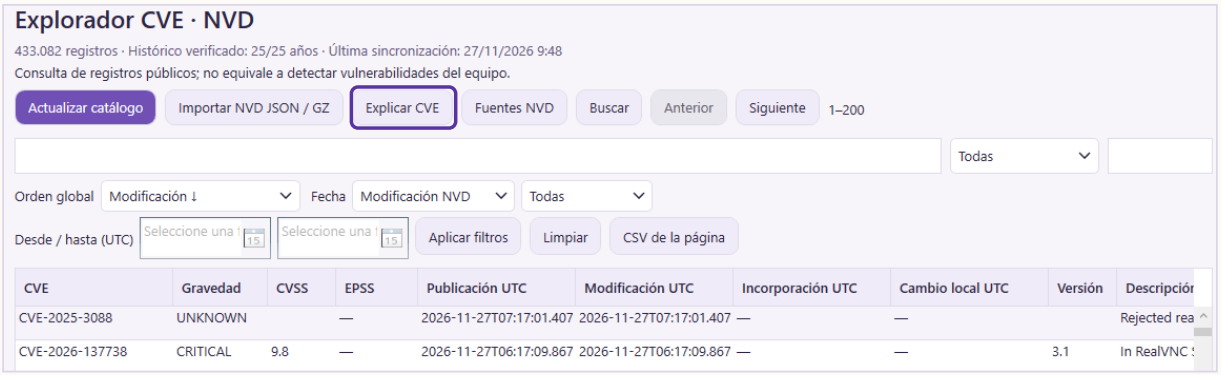


Figure 5. Explain CVE (shown as Explicar CVE) uses the selected row. For this walkthrough, look up CVE-2024-11477.

1. **Look up the identifier.** Open **CVE explorer**, enter **CVE-2024-11477** and select **Search**. Use **Limpiar** (Clear) to remove filters if needed.
2. **Select the record and choose Explain CVE.** WinCVE opens **AI assistant**, enters the ID and prepares the initial evidence. You can also enter the ID directly in the assistant.
3. **Choose a topic and provider.** Select **Mitigation and verification** and your configured provider. Choose **Prepare evidence** after changing the topic. For the local evidence sheet, choose **Offline evidence (no AI)**.
4. **Read the evidence and send the request.** Review **Evidence used by AI**. Select **Ask** and authorize the request if you are using a remote provider. The result appears in **Answer**.
5. **Verify and record the result.** Open the CERT-EU advisory and confirm the installed version. CERT-EU identifies 7-Zip 24.07 as the fixed release. Record the observed version, decision and evidence.

> **What the assistant uses**
>
> The evidence comes from the local catalog and includes available metrics, CPE criteria and references. WinCVE 2.0.5 asks AI models to respond in Spanish. Open the original references and check the advisory before acting.

Example review note

“CERT-EU identifies 7-Zip 24.07 as the fixed release. Check the installed version to confirm applicability. If remediation is needed, record the new version and run the inventory again.”

CERT-EU · 7-Zip advisory for this walkthrough ›

16 / ON-DEVICE INFERENCE

Local AI with Ollama and LM Studio

WinCVE 2.0.5 can use a model that runs on the same Windows computer. Start the local server and use the model ID it reports.

Ollama

1. **Install and open Ollama on Windows.** Keep the service running. Download **llama3.2** for this walkthrough. The initial download requires access to the Ollama model registry.

```powershell
ollama pull llama3.2
ollama list
```

2. **Connect from WinCVE.** In **Configurar IA › Proveedor**, select **Ollama · local**. WinCVE connects to **127.0.0.1:11434**. Choose **Cargar modelos** and select the installed model.
3. **Test it and use it in the assistant.** Select **Probar IA**. Once a reply appears, you can save the profile as your default and follow the CVE walkthrough on the previous page.

LM Studio

1. **Load a chat model in LM Studio.** In the **Developer** tab, use **Start server** to run the local server on **127.0.0.1:1234**.
2. **Choose LM Studio · local in WinCVE.** Load the model list, select the ID and choose **Probar IA**. WinCVE connects without a token. If your LM Studio instance requires authentication, choose a provider compatible with your environment.

> **Run a query with the installed model**
>
> Check that the model and server process the request locally. For the catalog evidence sheet alone, choose **Offline evidence (no AI)**.

Ollama · Windows documentation ›

LM Studio · Local API server ›

17 / COMMAND LINE

AI from PowerShell

The AI commands in **WINCVE_CLI.bat** prepare evidence from the local catalog. For a remote service, the CLI reads the provider's environment variable and requires **--allow-remote**.

Open the evidence sheet or query a local model

```powershell
$cve = 'CVE-2024-11477'
.\WINCVE_CLI.bat explain $cve --provider offline --topic 3
.\WINCVE_CLI.bat ai-models --provider ollama
.\WINCVE_CLI.bat explain $cve --provider ollama --model llama3.2 --topic 3
```

The first **explain** command displays the local evidence sheet. The second uses Ollama and requires a running service and an installed model on the same Windows computer.

Use OpenAI in a PowerShell session

```powershell
$key = Read-Host 'OpenAI API key' -AsSecureString
$env:OPENAI_API_KEY = [System.Net.NetworkCredential]::new('', $key).Password
.\WINCVE_CLI.bat ai-models --provider openai --allow-remote
$model = Read-Host 'Exact model ID'
.\WINCVE_CLI.bat ai-test --provider openai --model $model --allow-remote
$query = @('explain', $cve, '--provider', 'openai', '--model', $model,
           '--topic', '3', '--allow-remote', '--json')
.\WINCVE_CLI.bat @query
Remove-Item Env:OPENAI_API_KEY
Remove-Variable key
```

Set **$cve** as shown in the first example. **ai-test** sends a sample message. With **explain**, **--allow-remote** authorizes sending the CVE evidence to the selected provider.

--topic	Topic	--topic	Topic
1	Summary and scope	3	Mitigation and verification
2	Priority and exposure	4	Educational explanation

Run **ai-providers** to find the variable for each service, such as **OPENROUTER_API_KEY** for OpenRouter.

18 / AI ASSISTANT

Troubleshoot AI

First find the CVE in the catalog. Then check the provider connection and test whether the selected model can generate a reply.

Message or symptom	What to check in WinCVE 2.0.5
CVE not found	Confirm the ID in CVE explorer and check the catalog date. If the record is missing, update or import NVD data.
Ask is disabled	Select **Prepare evidence** after changing the CVE or topic. Wait for any ongoing operation to finish or cancel it.
HTTP 401	Check that the key belongs to the selected provider and project.
HTTP 403 or 404	Verify the key permissions, your access to the model and the exact model ID.
HTTP 402 or 429	Check your balance, billing, request limits and quota in the provider dashboard.
Models are listed but the test fails	Try a model that supports chat. Listing models and sending a chat request are separate operations.
Ollama or LM Studio does not respond	Confirm the service is running on this Windows computer and listening on the expected local port.

Profiles and API key recovery

Desktop profiles are stored in **data/ai-profiles.dpapi** and tied to your Windows account. **Olvidar clave** (Forget key) removes the credential from the profile. If you changed user or computer and the file cannot be opened, close WinCVE, preserve the file under a different name in a private location and configure the provider again.

> **Providers included in 2.0.5**
>
> Alongside Ollama and LM Studio, WinCVE supports OpenAI, OpenRouter, Anthropic Claude, Google Gemini, DeepSeek, Mistral AI, Groq and xAI Grok. Each remote service has its own API keys, model catalog and terms.

OpenAI · Managing ChatGPT and API billing ›

19 / WORKSPACE

Personalization and integrations

Open **Apariencia** (Appearance) on the top toolbar or **Personalization** in the sidebar to adjust WinCVE to your screen and workflow.

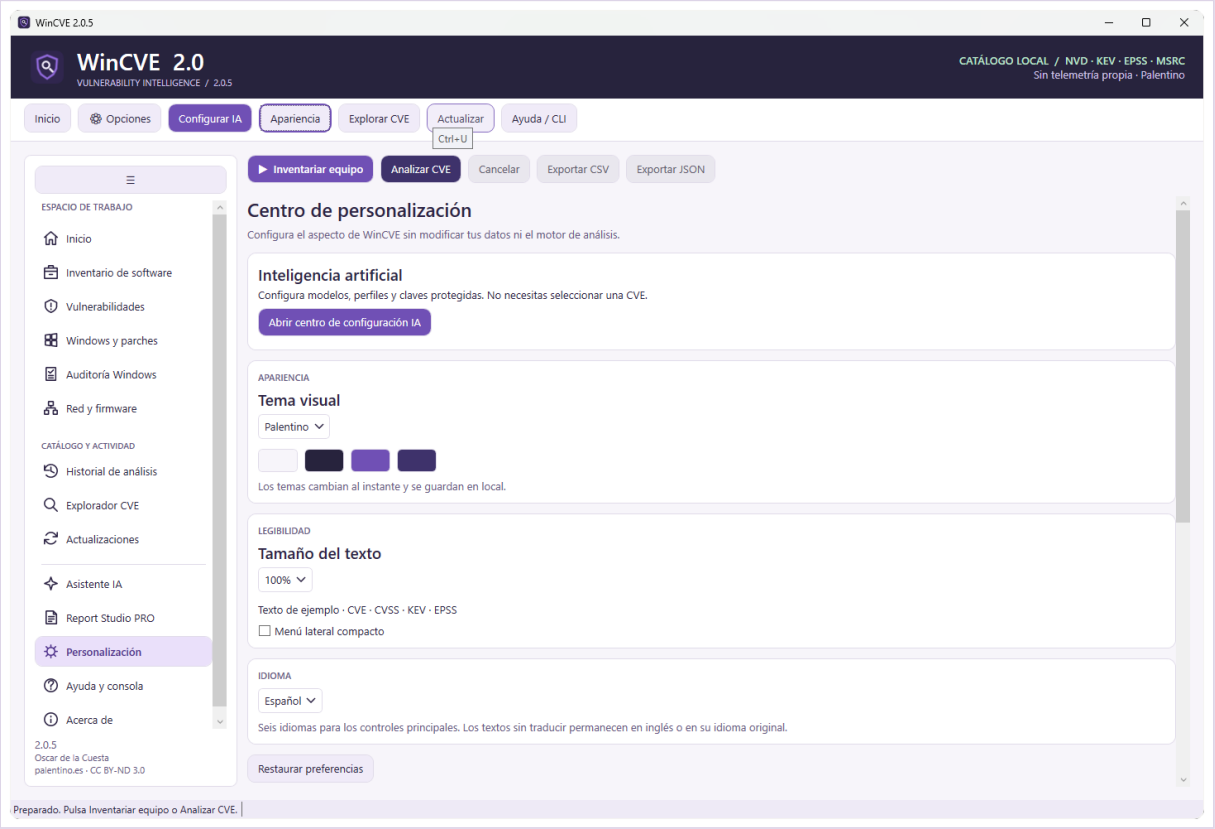


Figure 6. Personalization includes access to the AI Configuration Center.

Preference	Options
Visual theme	Palentino, Dark PRO, Light PRO, Cream, Cyber and Graphite.
Text size and navigation	Choose 90%, 100%, 110% or 120% text scaling. Turn on compact navigation for more room.
Application language	Choose English, Spanish, French, German, Italian or Portuguese. Select Auto / System to follow the Windows language if supported.

WinCVE saves these preferences for the next launch. Source records and some screens retain their original language.

PalClam and Modern Terminal AI. Options provides links to the Palentino websites and companion applications. Check whether they are installed or select their executable to open them.

20 / COMMAND LINE

Get started with the command line

Open PowerShell in the WinCVE folder that contains **WINCVE_CLI.bat**. You can query the local catalog without opening the desktop application.

```powershell
.\WINCVE_CLI.bat version
.\WINCVE_CLI.bat doctor
.\WINCVE_CLI.bat status --json
.\WINCVE_CLI.bat intel-status --json
.\WINCVE_CLI.bat cve CVE-2024-11477
.\WINCVE_CLI.bat help search
```

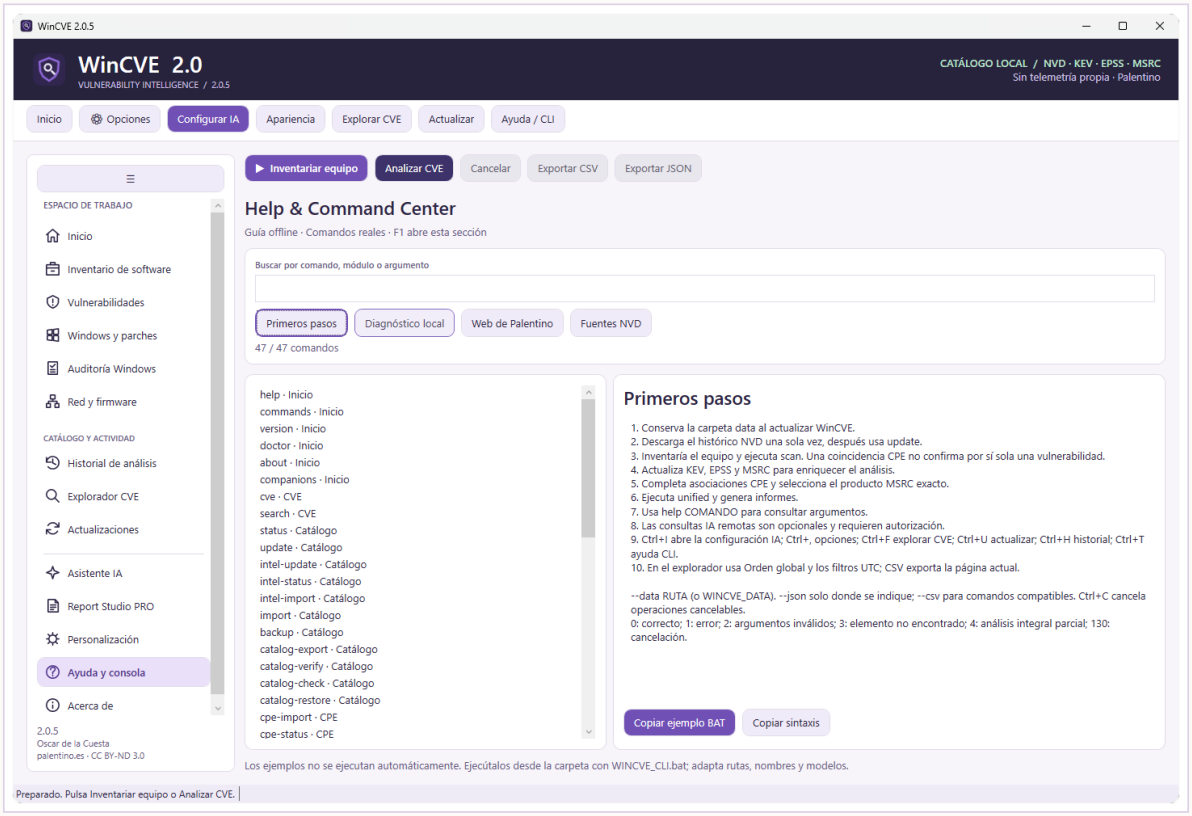


Figure 7. The Help & Command Center lets you search commands and copy their syntax and examples.

doctor checks local paths and files. **status** reads NVD coverage. **intel-status** shows the KEV and EPSS dates.

Press **F1** in the app or run **commands** from the console to see the 47 commands documented in version 2.0.5.

21 / POWERSHELL

Repeatable queries and tasks

Use explicit arguments to reproduce a query. Name your output files so you can identify the period or scan they cover.

Search by publication or modification date

```powershell
.\WINCVE_CLI.bat search "7-Zip" --sort published-desc --limit 20
.\WINCVE_CLI.bat search --date-field modified `
  --since 2026-11-01 --until 2026-12-01 --dates --limit 50
```

The second example finds November modifications in UTC. The **--until** boundary is exclusive. **--dates** includes the date columns in plain text output. Use **--json** for structured dates.

Save the inventory, findings and report

```powershell
.\WINCVE_CLI.bat inventory --json > inventory.json
.\WINCVE_CLI.bat scan --save --json > findings.json
.\WINCVE_CLI.bat unified --output unified-report.html
$LASTEXITCODE
```

scan --save saves the scan to history. In scripts, check **$LASTEXITCODE** immediately after each command. For a software-only HTML report, see **help report**.

Code	Meaning	Code	Meaning
0	Success	**3**	Item not found
1	Execution error	**4**	Partial unified assessment
2	Invalid arguments	**130**	Operation canceled

Confirm the data path

Set **--data PATH** or use **WINCVE_DATA**. The explicit argument takes precedence. Run **doctor** to verify which folder the console will use.

22 / COMMON COMMANDS

CLI quick reference

Run commands with **WINCVE_CLI.bat**. Use **help COMMAND** to see the full syntax for your copy of WinCVE.

Task	Commands	When to use them
Find commands	help, commands, version, doctor	Check syntax, the installed version and the local data path.
Query the catalog	cve, search, status, intel-status	Look up a CVE ID and verify coverage and dates.
Maintain the catalog	backup, catalog-check, catalog-export, catalog-verify	Back up and check the local catalog or verify a portable ZIP.
Refresh data sources	update, intel-update, windows-update	Update NVD, KEV and EPSS, or Microsoft MSRC releases, respectively.
Assess the computer	inventory, scan, audit, windows-inventory, windows-products	Review software, findings, settings, the Windows build and available MSRC products.
Look up CPE or firmware	cpe-status, cpe-search, device-list, firmware-scan	Find CPE mappings and assess a saved device profile.
Document results	report, unified, dashboard-history	Create a report or review the saved scan history.
Use AI	ai-providers, ai-models, ai-test, explain	List providers and models, test a connection and explain a CVE.

Three examples to copy

```powershell
.\WINCVE_CLI.bat commands --filter windows
.\WINCVE_CLI.bat search "7-Zip" --limit 50 --offset 50 --json
.\WINCVE_CLI.bat help catalog-restore
```

In **search**, an offset of 50 skips the first 50 results. Keep the filters, sort order and catalog version consistent when collecting multiple pages.

23 / MAINTENANCE

Back up, restore and migrate

Back up the data folder to recover an installation. To move just the vulnerability catalog, create a catalog ZIP in WinCVE.

Edition or setting	Usual data location
EXE installer	%LOCALAPPDATA%\Palentino\WinCVE\data
Portable ZIP	The data folder next to WinCVE.exe
Custom path	WINCVE_DATA for the application. The CLI also accepts --data.

Back up or migrate an installation

1. **Close the app and the CLI.** Check the data path in the app or with **doctor**. Copy the entire **data** folder to a private location to keep the databases, inventories and preferences.
2. **Back up before migrating.** Version 2.0.5 adds date fields and indexes to **cve.db**. Keep the original backup so you can return to the prior version. When opening 2.0.5, check the catalog and the data path.

Move the SQLite catalog

1. **Export and verify.** In **Updates › Portable catalog**, select **Create catalog ZIP**, then **Verify package**. WinCVE exports NVD, KEV, EPSS and a manifest.
2. **Restore on the destination computer.** In the same tab, select **Restore catalog / backup**. If a catalog already exists, verify the source and confirm replacement only if intended. WinCVE copies the previous catalog to **data/backups**.

```powershell
.\WINCVE_CLI.bat catalog-export catalog.zip
.\WINCVE_CLI.bat catalog-verify catalog.zip
```

> **Installation-specific data**
>
> Unknown local dates remain blank after migration. The public catalog ZIP leaves out local import timestamps. Use a private **data** backup to keep MSRC, the CPE dictionary and inventory data. Keep encrypted keys associated with the original Windows account.

24 / PRACTICAL EXAMPLES

Two end-to-end walkthroughs

The first walkthrough applies a public software advisory. The second moves an updated catalog to an offline Windows computer.

1. Review a 7-Zip advisory

1. **Find CVE-2024-11477.** Paste the identifier into CVE explorer. Open **Details** and **References**. The CERT-EU advisory documents the fix in 7-Zip 24.07.
2. **Identify the installed version.** Open **Software inventory**, find 7-Zip and confirm the version. For a portable copy, check the version in 7-Zip itself.
3. **Document the change and verify it.** If the installed version is affected, choose an up-to-date compatible release from the official channel. Record the old version, new version and advisory. Run the inventory again to confirm the change.

2. Prepare an offline workstation

1. **Update on a connected computer.** Check coverage and dates for NVD, KEV and EPSS. Create a catalog ZIP and verify it before transferring it with an approved method.
2. **Load the catalog on the offline computer.** Close any other WinCVE instances and restore the trusted package from **Portable catalog**. Check its coverage and repeat a known query in CVE explorer.
3. **Date the assessment.** Record when each source was synchronized. Run local correlation and note which modules and releases were available when you wrote the report.

Example 7-Zip remediation record

Field	Example
Product and original version	7-Zip 24.06 on an example computer.
Reference and criterion	CVE-2024-11477. CERT-EU 2024-118 documents the fix in 24.07.
Decision	Update to an approved release that includes the fix.
Closeout	Record the final observed version, verification date and owner.

Find the advisories and sources ›

25 / DIAGNOSTICS

Troubleshooting

Start by checking the WinCVE version, data path and catalog status. Use these steps to resolve common startup, search and update issues.

Symptom	Check and follow-up
The portable edition does not start	Check the architecture and SHA-256 hash. Extract the entire ZIP to a writable folder and run WinCVE.exe there.
Catalog empty or unavailable	Run **doctor** and **status**. Check the data path and free disk space. Import the bundled catalog or restore a trusted package.
Search returns no results	Select **Limpiar** (Clear), search for the full ID and check the CVE year, severity, UTC range and last sync.
Import dates are blank	The data may come from a published catalog or include records that predate 2.0.5. Use the NVD publication and modification dates when you need the source dates.
Update incomplete	Review the status message, connectivity and free disk space. Check source dates and avoid simultaneous writes to the same catalog.
No MSRC results	Check the months imported, exact product, edition, build and architecture. Open the Microsoft advisory to verify applicability.
AI test fails	Check the provider, model availability and key. Start the server for local AI. For remote AI, check authorization and connectivity.

If you build and package WinCVE

Missing KEV means the data being packaged contains no KEV records. From the project folder, run **ACTUALIZAR_TODO.bat** and review its NVD, intelligence and MSRC results. If only intelligence needs refreshing, **ACTUALIZAR_INTEL.bat** updates KEV and EPSS.

Use **WINCVE_CLI.bat intel-status --json** to confirm that both sources have records in the data path used by **PREPARAR_DISTRIBUCION.bat**. If the download fails, check the feed error or import the official files from the update center. Folders ending in **.incompleto** keep partial results for troubleshooting.

Find out where to report an issue ›

26 / REFERENCES

Sources and credits

WinCVE Explorer & Control Center is a Palentino project by Oscar de la Cuesta Campillo. This guide covers version 2.0.5 for Windows.

Project and support

Palentino · WinCVE website
Downloads by architecture, published SHA-256 hashes, screenshots and the Trust Center.

GitHub · v2.0.5 release
Public installer and portable packages.

GitHub · WinCVE issues
Include the version, architecture, edition, steps and exact message. Review any attachments before posting.

Intelligence and advisory sources

NIST NVD · Vulnerabilities and references
Vulnerability records, dates, severity and technical references.

NIST NVD · CPE dictionary
Standard names for products, systems and packages.

FIRST · CVSS standard
Specification for technical severity scoring.

CISA · Known Exploited Vulnerabilities
Catalog of vulnerabilities with known exploitation.

FIRST · Exploit Prediction Scoring System
Methodology and interpretation of EPSS probability.

Microsoft · Security Update Guide
Microsoft security advisories, products and updates.

CERT-EU · Advisory 2024-118 on 7-Zip
The advisory for CVE-2024-11477 used in the walkthrough.

Screenshots are from the Palentino gallery. Procedures were checked against the WinCVE 2.0.5 source code, README, CLI guide and changelog.

Project license · CC BY-ND 3.0 Unported
Dependencies and third-party data are subject to their own terms.