Security Whitepaper

Measure Killer v3.0.2 · Brunner BI GmbH · Zug, Switzerland

This document outlines the security details and data handling practices of Measure Killer. It is intended for IT and security professionals conducting vendor reviews.

Summary of requirements

All outbound connections made by Measure Killer. Connections marked Optional can be ignored if they are blocked or fail. Some connections are only needed for one kind of item or mode, as noted in their purpose. The domains below are for the commercial cloud. For the national clouds, see **Sovereign clouds**.

DOMAIN	PURPOSE	PORT	PROTOCOL
`login.microsoftonline.com`	Sign-in with Microsoft Entra ID (all online modes)	443	HTTPS
`api.powerbi.com`	All Power BI REST API calls (listed below) and XMLA connections to semantic models (powerbi://api.powerbi.com)	443	HTTPS
`*.pbidedicated.windows.net`	XMLA connections to semantic models in the Power BI Service. Microsoft requires this domain for XMLA connections (see XMLA endpoint connection)	443	HTTPS
`api.fabric.microsoft.com`	All Fabric REST API calls (listed below)	443	HTTPS
`*.datawarehouse.fabric.microsoft.com (older items: *.datawarehouse.pbidedicated.windows.net)`	SQL connections to the SQL analytics endpoints of Lakehouses, Warehouses and Fabric SQL databases. Only needed to analyze these items	1433	TDS (the Microsoft SQL Server protocol), encrypted with TLS
`onelake.dfs.fabric.microsoft.com`	Fabric OneLake. Needed for some Fabric items	443	HTTPS
`*.asazure.windows.net`	XMLA connections to Azure Analysis Services. Only needed in the Analysis Services modes	443	HTTPS
`Your SQL Server Analysis Services server`	XMLA connections to the on-premises Analysis Services server you enter. Only needed in the Analysis Services modes	2383 (default instance), 2382 (SQL Server Browser) and the instance port for named instances	TCP
`measurekillerlicense-hrbvcncabnddawb7.switzerlandnorth-01.azurewebsites.net`	License verification and app information (latest version and start-up message). Required for all modes that need a license	443	HTTPS
`cdn.plot.ly` Optional	The plotly.js chart library used by the charts in Measure Killer. If it is blocked, the charts are not displayed	443	HTTPS

The local modes connect only to the Power BI Desktop instance running on your own machine (localhost). These connections never leave your machine.

Measure Killer 3.0 and later no longer contact `*.servicebus.windows.net`, `www.measurekiller.com`, `brunner.bi`, `raw.githubusercontent.com`, `postman-echo.com`, `time.windows.com`, `pool.ntp.org`, `microsoft.com`, `cloudflare.com` or `ifconfig.me`. Earlier versions used them for license verification, the version check and the start-up message.

Sovereign clouds

In **Settings > Sovereign cloud**, the Power BI, sign-in and XMLA addresses can be switched to a national cloud. The presets use these domains instead of `api.powerbi.com` and `login.microsoftonline.com`:

CLOUD	POWER BI	SIGN-IN
US Government (GCC)	`api.powerbigov.us`	`login.microsoftonline.com`
US Government (GCC High)	`api.high.powerbigov.us`	`login.microsoftonline.us`
US Government (DoD)	`api.mil.powerbigov.us`	`login.microsoftonline.us`
China	`api.powerbi.cn`	`login.chinacloudapi.cn`

The Fabric API, OneLake, license service and cdn.plot.ly addresses are the same in every cloud.

Data handling and privacy

Metadata-only interaction

Measure Killer only interacts with **metadata** from Power BI Desktop or the Power BI Service. At no point does Measure Killer read, store, or process actual data contained within Power BI reports or models. This strict limitation to metadata ensures that sensitive data remains confidential and secure.

Beyond Power BI related data, Measure Killer needs to collect the following metadata for license verification (see also **License metadata**): installed Measure Killer version, Windows user name, computer name and license key.

What is considered metadata?

- Names of artifacts (reports, semantic models, workspaces, users/email addresses)
- DAX and M expressions including comments
- Names of measures, tables, calculated columns, calculated tables, calculation groups, field parameters, etc.
- Uncompressed size of columns
- All definitions (e.g. name of reports, pages, visuals, visual titles, visual size and other metadata)
- Names and data types of the tables, views and columns of Lakehouses, Warehouses and Fabric SQL databases

Local processing

All processing and analysis of metadata is performed locally on the user's machine through the installed client software. The operations on metadata do not involve or require any external processing or storage facilities. There is no database that is hosted, managed, or used to process any kind of information. Everything is done on the user's machine and not transmitted anywhere besides REST API, XMLA or SQL connections with Microsoft directly.

XMLA endpoint connection

To retrieve metadata from semantic models in the Power BI Service, XMLA endpoints are used. The Analysis Services modes use XMLA connections to Azure Analysis Services or SQL Server Analysis Services in the same way. Measure Killer uses Microsoft's Analysis Services client libraries (ADOMD.NET and AMO/TOM, version 19.107.2) for these connections. Authentication happens via the entered Microsoft account (ADOMD client).

Microsoft requires connections to `*.pbidedicated.windows.net` on port 443 for XMLA connections to the Power BI Service (Microsoft Learn: "Troubleshoot XMLA endpoint connectivity").

SQL endpoint connection

To analyze Lakehouses, Warehouses and Fabric SQL databases, Measure Killer reads the names and data types of their tables, views and columns from the SQL analytics endpoint. The connection uses Microsoft's mssql-python driver on port 1433. It is always encrypted, and the server certificate is validated. It authenticates with the user's Microsoft Entra access token. Measure Killer only queries the system catalog views (`sys.schemas` , `sys.tables` , `sys.views` , `sys.columns` and `sys.types`). It never queries the tables themselves.

Online / offline modes

Local modes ("Single model" and "Shared model on local machine"): connect to the local instance of Analysis Services that Power BI Desktop runs, to retrieve the metadata they need. These modes do not need a license. The only interactions with the internet are at launch (license verification and app information, see **License verification**) and the plotly.js chart library when charts are shown.

Analysis Services modes: connect to the Azure Analysis Services or SQL Server Analysis Services server that you enter, or that a scan of your tenant finds.

Online modes (the developer modes, the admin modes, Tenant Analysis and Limited Tenant Analysis): need a valid license and an internet connection. External connections are REST API calls and XMLA and SQL connections to Microsoft, as outlined above.

"MK Automation" opens the Measure Killer automation web page in your default browser. Measure Killer does not update itself. Links such as "Download" or "Request a demo" also open in your default browser.

Authentication

Users sign in with their own Microsoft Entra ID account (delegated permissions), through Microsoft's azure-identity library. Two sign-in methods can be chosen in Settings: interactive browser sign-in (the default) and device code sign-in.

- By default, sign-in uses Microsoft's public Azure CLI client application (ID `04b07795-8ddb-461a-bbee-02f9e1bf7b46`), so no app registration is needed in your tenant. The setting "Use new app registration for Measure Killer (Preview)" switches to Measure Killer's own multi-tenant app registration (ID `dd810d9b-20b4-4b1f-b15b-1e9948ceba85`).
- No service principals, client secrets, certificates or passwords are used.
- Measure Killer requests the Power BI service scope (`https://analysis.windows.net/powerbi/api/.default`). It is used for the Power BI and Fabric API calls and for the SQL endpoint connections. Measure Killer also requests the Azure Storage scope (`https://storage.azure.com/.default`) for OneLake.
- During interactive browser sign-in, azure-identity opens a temporary listener on localhost (the first free port between 8400 and 8999) to receive Microsoft's sign-in redirect. It closes right after the sign-in, or after 5 minutes. Device code sign-in opens no port. This is the only port Measure Killer listens on, and Measure Killer runs no server.
- Access tokens are kept in memory only. They are not written to disk and not stored in saved .measurekiller files.
- XMLA connections authenticate through Microsoft's ADOMD.NET client (see **XMLA endpoint connection**).

Changes Measure Killer can make

Measure Killer only reads metadata, unless a user starts one of these actions:

Removing or hiding unused objects ("Kill", "Hide", "Restore" and "1-click cleanup"). These actions change the semantic model. In the Power BI Service they use the XMLA endpoint in read-write mode, so they need a Premium or Fabric capacity with XMLA read-write enabled, and write permission on the model. Measure Killer asks for confirmation before it writes to a model in the service. In the local modes, the changes go to the model open in Power BI Desktop. The .pbix file only changes when you save it in Power BI Desktop.

Managing workspace access (Fabric administrators only). Measure Killer can add the signed-in administrator to workspaces it needs to analyze, after asking for confirmation, and offers to remove that access afterwards. The "Workspace access" window can add or remove users and groups on workspaces (see Admin - Groups AddUserAsAdmin and Admin - Groups DeleteUserAsAdmin in the list of REST API calls).

Measure Killer never creates, deletes or refreshes items, and never changes reports. It never overwrites .pbix or .pbip files: exports are written as new files.

API endpoints and security measures

Secure requests (**HTTPS**) are made to Power BI and Fabric API endpoints, ensuring data in transit is encrypted.

Access tokens are securely passed in request headers, with responses parsed as JSON for internal processing.

Server certificates are always validated. Measure Killer trusts the root certificates of the Windows certificate store and of the certifi package. Python also rejects certificates issued with known compromised CA keys. A proxy and an extra CA certificate file can be set in Settings.

App information, such as the start-up message and the latest version, is fetched from the Measure Killer license service over HTTPS. The response is signed and checked (see **Version check and user notification**).

License verification

Measure Killer verifies a license with one HTTPS POST request to its license service (`measurekillerlicense-hrbvcncabnddawb7.switzerlandnorth-01.azurewebsites.net`, hosted on Azure in Switzerland North). This happens at every launch when a license key is entered. A minimal set of license-related metadata is sent (see **License metadata**).

The service decides whether the license is valid, expired or blocked.

If the license service cannot be reached, the licensed modes stay disabled for that session. There is no offline grace period. The local modes work without a license.

The legacy license verification method was removed in version 3.0. Measure Killer no longer contacts time servers (NTP or HTTPS), IP lookup services, Azure Event Hubs or blacklist downloads.

License metadata

For the purpose of validating active licenses and ensuring compliance, Measure Killer transmits a minimal set of license-related metadata to the license service. The request contains only the license key, the installed Measure Killer version, the Windows user name and the computer name. The public IP address is no longer collected. No Power BI metadata, report content, or user data is ever included in this process. All data is sent exclusively over encrypted channels (HTTPS).

`measurekillerlicense-hrbvcncabnddawb7.switzerlandnorth-01.azurewebsites.net` · port 443 · HTTPS

Version check and user notification

At every launch, Measure Killer fetches app information from the same license service with a GET request that sends no data. The information contains the latest version, the start-up message and the links shown in the app. The response is signed and checked. If the service cannot be reached, or the signature does not match, Measure Killer shows a default start-up text. Measure Killer does not download or install updates itself: the download link opens in your default browser.

REST API calls

REST API calls are made to Microsoft's Power BI and Fabric APIs for the acquisition of metadata. Authentication happens via Microsoft Entra ID (see **Authentication**). Once metadata has been acquired, all subsequent analyses and operations are carried out locally.

Some calls use POST but only read: PostWorkspaceInfo starts a metadata scan, Execute Queries reads model metadata, and the Get Definition calls return item definitions. Microsoft defines these calls as POST. The only calls that change your tenant are marked **(changes workspace access)**, see **Changes Measure Killer can make**.

Power BI REST API

API	METHOD	ENDPOINT
Groups - Get Groups	GET	`https://api.powerbi.com/v1.0/myorg/groups`
Groups - Get Group Users	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/users`
Capacities - Get Capacities	GET	`https://api.powerbi.com/v1.0/myorg/capacities`
Datasets - Get Datasets In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/datasets`
Datasets - Get Refresh History In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/datasets/{dataset.id}/refreshes`
Datasets - Get Refresh History	GET	`https://api.powerbi.com/v1.0/myorg/datasets/{dataset.id}/refreshes`
Datasets - Get Refresh Schedule In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/datasets/{dataset.id}/refreshSchedule`
Datasets - Get Refresh Schedule	GET	`https://api.powerbi.com/v1.0/myorg/datasets/{dataset.id}/refreshSchedule`
Datasets - Execute Queries In Group	POST	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/datasets/{dataset.id}/executeQueries`
Reports - Get Reports In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/reports`
Reports - Get Datasources In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/reports/{report.id}/datasources`
Reports - Get Datasources	GET	`https://api.powerbi.com/v1.0/myorg/reports/{report.id}/datasources`
Reports - Export Report In Group	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/reports/{report.id}/Export` (paginated reports only)
Reports - Export Report	GET	`https://api.powerbi.com/v1.0/myorg/reports/{report.id}/Export` (paginated reports only)
Dataflows - Get Dataflows	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/dataflows`
Dataflows - Get Dataflow Transactions	GET	`https://api.powerbi.com/v1.0/myorg/groups/{workspace.id}/dataflows/{dataflow.id}/transactions`
Apps - Get Apps	GET	`https://api.powerbi.com/v1.0/myorg/apps`
Apps - Get Reports	GET	`https://api.powerbi.com/v1.0/myorg/apps/{app.id}/reports`

Power BI Admin REST API

API	METHOD	ENDPOINT
Admin - Groups GetGroupsAsAdmin	GET	`https://api.powerbi.com/v1.0/myorg/admin/groups?$expand=users&$filter={filter}&$top={top}&$skip={skip}`
Admin - Users GetUserArtifactAccessAsAdmin	GET	`https://api.powerbi.com/v1.0/myorg/admin/users/{user.id}/artifactAccess?artifactTypes=Workspace`
Admin - WorkspaceInfo PostWorkspaceInfo	POST	`https://api.powerbi.com/v1.0/myorg/admin/workspaces/getInfo?lineage=true&datasourceDetails=true&getArtifactUsers=true`
Admin - WorkspaceInfo GetScanStatus	GET	`https://api.powerbi.com/v1.0/myorg/admin/workspaces/scanStatus/{scan.id}`
Admin - WorkspaceInfo GetScanResult	GET	`https://api.powerbi.com/v1.0/myorg/admin/workspaces/scanResult/{scan.id}`
Admin - Get Capacities As Admin	GET	`https://api.powerbi.com/v1.0/myorg/admin/capacities`
Admin - Get Activity Events	GET	`https://api.powerbi.com/v1.0/myorg/admin/activityevents?startDateTime={start}&endDateTime={end}&$filter={filter}`
Admin - Reports GetReportSubscriptionsAsAdmin	GET	`https://api.powerbi.com/v1.0/myorg/admin/reports/{report.id}/subscriptions`
Admin - Apps GetAppsAsAdmin	GET	`https://api.powerbi.com/v1.0/myorg/admin/apps?$top={top}`
Admin - Apps GetAppUsersAsAdmin	GET	`https://api.powerbi.com/v1.0/myorg/admin/apps/{app.id}/users`
Admin - Groups AddUserAsAdmin (changes workspace access)	POST	`https://api.powerbi.com/v1.0/myorg/admin/groups/{workspace.id}/users`
Admin - Groups DeleteUserAsAdmin (changes workspace access)	DELETE	`https://api.powerbi.com/v1.0/myorg/admin/groups/{workspace.id}/users/{user}`

Fabric REST API

API	METHOD	ENDPOINT
Items - List Items	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/items`
Items - List SQL Databases	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/sqlDatabases`
Items - Get Connection String (SQL endpoint)	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/sqlEndpoints/{sqlEndpoint.id}/connectionString`
Items - Get Warehouse	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/warehouses/{warehouse.id}`
Items - Get Item Definition	POST	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/items/{item.id}/getDefinition`
Items - Get Notebook Definition	POST	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/notebooks/{notebook.id}/getDefinition`
Long Running Operations - Get Operation State	GET	`https://api.fabric.microsoft.com/v1/operations/{operation.id}`
Long Running Operations - Get Operation Result	GET	`https://api.fabric.microsoft.com/v1/operations/{operation.id}/result`
Job Scheduler - List Item Job Instances	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/items/{item.id}/jobs/instances`
Job Scheduler - List Item Schedules	GET	`https://api.fabric.microsoft.com/v1/workspaces/{workspace.id}/items/{item.id}/jobs/{jobType}/schedules`

Fabric Admin REST API

API	METHOD	ENDPOINT
Tenants - List Tenant Settings	GET	`https://api.fabric.microsoft.com/v1/admin/tenantsettings`
Domains - List Domains	GET	`https://api.fabric.microsoft.com/v1/admin/domains`
Domains - List Domain Workspaces	GET	`https://api.fabric.microsoft.com/v1/admin/domains/{domain.id}/workspaces`

Security testing approach

We use a combination of automated scanning and testing along with manual reviews to check Measure Killer's security before and after each release:

Software composition analysis: when we begin development on a new version, we check all open-source dependencies for known vulnerabilities using pip-audit and OSS Index. Because many issues can be resolved by library updates, we track each new release. We then review any security fixes and confirm compatibility with Measure Killer. If it is stable and relevant, we incorporate it into our codebase.

Static code analysis: we run automated static analysis with tools such as Bandit (a Python security analyzer) and PyLint (for code quality and style). These tools flag potential security weaknesses. Our developers then review each flagged item to determine if it represents a real vulnerability or a false positive.

Automated testing and code review: we use pytest for extensive unit and integration testing. Security-wise, our tests focus on validation and parsing logic (ensuring .pbix and .rdl files are parsed securely), user authentication (verifying usage of the azure.identity library and tabular connections), error handling and fail-safe behavior (simulating network or parsing failures using mocks, and testing responses to Power BI API errors) and regression testing (checking that known issues from previous Measure Killer versions remain fixed).

Build and code signing

Exact versions: every release is built from a lock file that pins the exact version of every third-party package. The build stops if the build environment holds any other package.

Python runtime: Measure Killer bundles Python 3.13.18. python.org publishes Python 3.13 security releases as source code only, without a Windows installer. We build Python from the official source code, after checking the download's Sigstore signature, with the build command that python.org uses for its own Windows releases. The OpenSSL libraries inside it are the ones signed by the Python Software Foundation.

Code signing: Measure Killer.exe and Measure Killer's own compiled libraries (.pyd and .dll files) are signed with Brunner BI GmbH's Extended Validation (EV) code signing certificate, issued by GlobalSign, and timestamped. Third-party files keep their vendors' signatures where they have one.

Rapid response to new vulnerabilities

If a vulnerability is discovered, our team follows a quick release process to track the issue, apply a prompt fix, and release an updated version of Measure Killer. We typically release bug-fix or patch versions on a monthly basis.

These measures, combined with our architecture that avoids storing or processing actual data, are designed to protect sensitive information and maintain a high level of security for all Measure Killer users.

Known CVEs — Python 3.13.18

The CVEs below were checked on 3 and 4 November 2026 against the versions bundled with Measure Killer 3.0.2. Python 3.13.18 is the latest Python 3.13 release and was checked against the Python Software Foundation advisories. It fixes every published Python CVE except the ones below. This includes CVE-2026-115557: Python now rejects certificates issued with the compromised certificate keys of eMudhra (emSign).

CVE	SEVERITY	ISSUE	MEASURE KILLER STATUS
`CVE-2026-115506, CVE-2026-118370`	**High** High (CVSS 8.7 and 8.2)	XML parser denial of service in the bundled Expat 2.9.0 (CWE-776, CWE-190). A crafted XML file can make the XML parser use a lot of CPU, or crash it. CVE-2026-118370 needs an XML element with more than a billion attributes, so a file of several gigabytes. Both are fixed in Expat 2.10.0 (2 November 2026), which no Python release contains yet.	Low risk. The app reads XML only from .rdl and .xlsx files you open, and from paginated report definitions it downloads from Power BI. The worst case is a hang or crash while it reads that file. No data is exposed. See also libxml2 and Expat below.
`CVE-2026-113351, CVE-2026-117610`	**High** High (CVSS 8.2)	Expat parser reset and external entity bugs (CWE-909, CWE-476). Expat can crash when a parser is reset, or while it parses an external entity.	Not applicable. The XML parser of Python that Measure Killer uses (ElementTree) never resets a parser and never parses external entities.
`CVE-2026-103995, CVE-2026-116566`	**Medium** Low (CVSS 2.0) and Medium (CVSS 5.3)	HTTP response lengths and host names with null bytes (CWE-444, CWE-158). Python accepts some malformed length values in HTTP responses, and host names that contain null bytes. Neither is fixed in any Python 3.13 release yet.	Low risk. The app only calls the fixed HTTPS addresses listed in this document. A malformed response would have to come from inside the encrypted connection to one of them.
`CVE-2026-27171, CVE-2026-34743, CVE-2026-42250`	**Medium** Low to Medium	zlib, xz and bzip2: bugs in compression libraries bundled with Python.	Not applicable. The affected functions are not part of Python's modules, or Python never calls them.
`CVE-2025-15367, CVE-2023-36632`	n/a	Parts of Python that Measure Killer does not use: POP3 (poplib) CVE-2025-15367, email CVE-2023-36632 (disputed).	Not applicable. These CVEs are in modules that Measure Killer never calls.
`CVE-2015-5652`	**High**	Untrusted Search Path on Windows (DLL hijacking). The python.exe on Windows can load a trojan readline.pyd from the current working directory.	Not applicable. The app ships no python.exe and never imports readline. See the mitigations below.

CVE-2015-5652, further mitigations in the Measure Killer desktop app:

The app does not use the system Python interpreter. PyInstaller (the package used to bundle the tool's .exe) loads python313.dll from the app's own installation folder, with a fixed module search path that does not include the current folder.

The only Windows DLL the app loads by name is kernel32.dll, a Windows system DLL that always loads from System32. Microsoft's Analysis Services libraries are loaded by their full path in the installation folder.

Measure Killer.exe and Measure Killer's own compiled libraries are code signed to help Windows SmartScreen and corporate EDR tools detect unsigned or tampered binaries.

For extra security, use the admin installer, where the default install is in Program Files (read and execute only). This prevents writing malicious DLLs to the installation folder.

Known CVEs — bundled libraries

LIBRARY	STATUS IN MEASURE KILLER
V8 and Chromium (Qt WebEngine 6.11.2: Chromium 140, with security patches up to Chromium 151)	V8 and the Chromium browser engine are bundled with the Qt WebEngine library. Measure Killer uses it only for its own pages: the charts (for example in the "Plot results" tab) and the lineage graph. Measure Killer builds these pages from your metadata, and names are escaped so they cannot turn into code. The lineage graph is a self-contained local page. The charts load one external file: the plotly.js library from cdn.plot.ly. The page pins the exact hash of that file (Subresource Integrity), so the browser refuses a changed file. Measure Killer never opens other websites inside the app: links open in your default browser. Because no untrusted content is processed, we are not aware of a way to exploit these vulnerabilities in Measure Killer.
LLVM	LLVM is part of opengl32sw.dll, a software OpenGL renderer that Qt ships for computers without a working graphics driver. Qt only loads it as a fallback. Its LLVM compiler only processes graphics code generated by Qt itself. Measure Killer does not compile or handle external code, so we are not aware of a way to attack Measure Killer through LLVM.
OpenSSL 3.5.9	Bundled with the Python interpreter as libcrypto-3.dll and libssl-3.dll, both signed by the Python Software Foundation. Measure Killer uses OpenSSL for only two things: outbound HTTPS connections to pre-determined API endpoints and reading certificates from the Windows certificate store. It never opens password-protected certificate files (.pfx/.p12), never handles secure message formats (CMS/PKCS#7), never uses DTLS or the Certificate Management Protocol (CMP), and never acts as a server. The SQL endpoint and Analysis Services connections use the Windows TLS stack through Microsoft's drivers, not OpenSSL. **No known CVE affects OpenSSL 3.5.9** (checked on 4 November 2026 against the OpenSSL vulnerability list for version 3.5). It fixes all CVEs published up to the OpenSSL advisory of 29 September 2026, including CVE-2026-35189 (excessive memory use for CRL distribution points), the only recent OpenSSL CVE that could have affected Measure Killer.
libxml2 2.11.9 and Expat 2.9.0	CVEs associated with libxml2 and Expat typically become relevant if an application processes malformed or hostile XML from unknown sources. Measure Killer parses XML only with Expat (part of Python), and only these files: .rdl files created by Power BI Report Builder, Microsoft Report Builder, or generated via Power BI's "Export Report In Group" API, and the pivot table parts of an "Analyze in Excel" .xlsx file you select. libxml2 (through the lxml package) is only used to write Excel exports and never parses input. These files have a defined structure and come from you or from Microsoft's API, making the known XML-related exploits not applicable. See also the Expat CVEs in the Python section.
libvpx and libaom	These video codecs are part of the Chromium engine inside Qt WebEngine. Measure Killer's pages contain no video or audio, and Qt's multimedia playback is not used. Potential vulnerabilities in these libraries (usually triggered by malformed video content) do not pose a risk in our application.
Qt 6.11.2	Qt provides the main user interface framework. Qt's published vulnerabilities for 6.11.2 concern network access (QNetworkAccessManager), CBOR and JSON parsing, vector images, and modules Measure Killer does not ship. Measure Killer does not use these features: its network calls go through Python, not Qt. While Qt can load external HTML or JavaScript, Measure Killer does not permit loading unknown URLs or scripts. Similar to V8, we only use Qt WebEngine for pages generated internally by the tool.
Skia (Chromium 140, with security patches up to Chromium 151)	Skia is an image rendering engine used indirectly by Qt WebEngine. We do not load or display arbitrary images in Measure Killer, only predefined icons and resources stored locally. With no untrusted image handling, Skia-related exploits are not a concern.
SQLite3 3.50.4	Measure Killer uses SQLite to store activity logs of the Power BI tenant, such as activity events, report views and capacity metrics, in a local database file. We do not open or process any external .sqlite files. SQLite 3.50.4 is affected by CVE-2026-11822 and CVE-2026-11824 (fixed in SQLite 3.53.2), and by CVE-2026-119371, CVE-2026-119373 to CVE-2026-119378 and CVE-2026-119591 (fixed in SQLite 3.54.0). Their severity ranges from Low to High. Each one needs a crafted database file or crafted SQL. Low risk for Measure Killer: the app runs only its own SQL, with values passed as parameters, on its own database file in your user folder. Python 3.13.18 still bundles SQLite 3.50.4.

Known CVEs — other libraries

LIBRARY	STATUS IN MEASURE KILLER
certifi (2026.7.22)	The list of trusted root certificates. Advisory GHSA-6q48-6c7w-9gw2 (Critical) concerns the emSign root whose intermediate keys were compromised. Mitigated: Python 3.13.18 rejects certificates issued with those keys, whichever root certificate they chain to (CVE-2026-115557).
urllib3 (2.7.0)	CVE-2026-97687 (HTTPS proxy TLS settings ignored) does not apply, because the app never uses that proxy mode. CVE-2026-97688 and CVE-2026-97689 (endless loop or high memory use on chunked responses) need a malicious server. Measure Killer only connects to the endpoints listed in this document.
PyJWT (2.13.0)	Measure Killer only uses PyJWT to read claims from the Microsoft access token it received over HTTPS. It does not use PyJWT to validate tokens. CVE-2026-101918 and CVE-2026-102265 (crash on a crafted token) need a token from an attacker, but the token comes from Microsoft over HTTPS. The other PyJWT advisories need signature checks, which the app does not use.
cryptography (50.0.0, with its own OpenSSL 4.0.1)	Only used to check the answers of the Measure Killer license service. The app uses this package for nothing else. The known OpenSSL 4.0.1 CVEs are in other features (such as QUIC, DTLS, CMS, CMP, TLS and signing) and do not affect this use.
No published advisories	None were found for requests, msal, azure-identity, mssql-python and its ODBC driver 18.6.2.1, pandas, numpy, openpyxl, plotly, PyInstaller, Microsoft's Analysis Services client libraries and the other bundled libraries.