

The Kaspersky logo, consisting of the word "kaspersky" in a lowercase, bold, sans-serif font. The background of the slide features a large white hexagonal shape with rounded corners, set against a teal-to-green gradient background.

kaspersky

Release Notes for Kaspersky Vulnerability Management 1.0

© 2026 AO Kaspersky Lab

Contents

[Kaspersky Vulnerability Management 1.0](#)

Release Notes for Kaspersky Vulnerability Management 1.0

The intended purpose of Kaspersky Vulnerability Management (hereinafter also referred to as the "solution") is vulnerability management in the IT infrastructure of an organization.

Kaspersky Vulnerability Management:

- Provides information about the assets of the organization's IT infrastructure
- Performs vulnerability scanning on assets
- Analyzes asset compliance with internal, industry and regulatory security requirements
- Provides the means to analyze and prioritize detected vulnerabilities
- Provides a public API that allows third-party systems to receive data about assets and detected vulnerabilities

HARDWARE AND SOFTWARE REQUIREMENTS

Minimum hardware requirements

The minimum hardware requirements for the device on which you plan to install Kaspersky Vulnerability Management components are listed in the table below.

Minimum hardware requirements

Number of assets	Installation option	
	All on one device Kaspersky Vulnerability Management components, including the DBMS, and Kaspersky Security Center components are installed on the same device.	Kaspersky Vulnerability Management installed separately Kaspersky Vulnerability Management components, including the DBMS, are installed separately from the Kaspersky Security Center components.
1–1000	• CPU: 16 cores, 2.5 GHz • RAM: 24 GB • Free disk space: 300 GB • Disk performance, IOPS: 1000	• CPU: 12 cores, 2.5 GHz • RAM: 16 GB • Free disk space: 200 GB • Disk performance, IOPS: 1000
1001–10000	• CPU: 20 cores, 2.5 GHz • RAM: 48 GB • Free disk space: 600 GB • Disk performance, IOPS: 1000	• CPU: 16 cores, 2.5 GHz • RAM: 32 GB • Free disk space: 400 GB • Disk performance, IOPS: 1000

Software requirements

Kaspersky Vulnerability Management components can be installed on a device running one of the following operating systems:

- ALT Server 10 64-bit
- RED OS 8 64-bit
- Astra Linux Common Edition (operational update 2.12) 64-bit

This operating system is not supported in the closed software environment mode.

- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8) 64-bit, also in closed software environment mode
- Debian 11.x 64-bit
- Platform V SberLinux OS Server (SLO) 8.10.1 64-bit
- Platform V SberLinux OS Server (SLO) 9.5.1 64-bit
- Ubuntu Server 22 64-bit

Kaspersky Security Center Network Agent supports the Kaspersky Vulnerability Management functionality in the following operating systems:

- ALT Server 10 64-bit
- RED OS 8 64-bit
- Astra Linux Common Edition (operational update 2.12) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8) in closed software environment mode 64-bit
- CentOS Stream 10 64-bit
- Red Hat Enterprise Linux Server 10 64-bit
- Rocky Linux 9.x 64-bit
- Ubuntu Server 22 64-bit
- Ubuntu Server 24 64-bit
- Windows 10 32-bit/64-bit
- Windows Server 2025 64-bit

One of the following database management systems can be used for the solution's database:

- PostgreSQL 15, 16, 17, 18
- Postgres Pro 18
- Postgres Pro Certified 18

Supported versions of Kaspersky Security Center and Network Agent

Kaspersky Vulnerability Management supports Kaspersky Security Center Linux Administration Server, Kaspersky Security Center Web Console, and Network Agent 16.3.

The current version of Kaspersky Vulnerability Management does not support the Kaspersky Security Center Linux Administration Server installed as a high-availability cluster.

For hardware and software requirements of the Kaspersky Security Center Administration Server, Kaspersky Security Center Web Console, and the Network Agent, see the [Kaspersky Security Center Help](#).

DEPLOYING THE SOLUTION

For information about the deployment of Kaspersky Vulnerability Management, see the [solution Help](#).

KNOWN LIMITATIONS

Kaspersky Vulnerability Management has some limitations that are non-critical for the operation of the solution:

- For some vulnerabilities detected as a result of the *Agentless black-box scanning* task, only limited information is displayed.
- Copying, moving, pausing, and resuming Kaspersky Vulnerability Management tasks is not supported.
- The results of the *Agentless black-box scanning* task are displayed after the background tasks have been processed by the service, which takes some time. You can speed up the processing of results by enabling the **Process results immediately after task completion** setting in the advanced task settings.
- To obtain information about software installed on a Windows asset, the Network Agent must be installed on the asset.
- In the cards of software installed on Linux assets, on the **Installed on assets** tab, the **Path to file** field is not filled.
- Asset groups are not supported in data collection scopes for reports.

- The scope of a role for Kaspersky Vulnerability Management is not limited, even if combinations of administration groups and users have been added in the scope of the role.
- If a Kaspersky Vulnerability Management session is active and the set of permission for that session's user account is changed, the changes take effect with a lag of up to five minutes.
- In the properties of Kaspersky Vulnerability Management tasks, on the **Results** tab, for events for the *Completed with warning* task status, the **Description** field is not filled.
- White-box scanning can be performed only on Linux assets.
- When scanning RED OS assets for compliance with profiles containing a rule that verifies that the automatic file system mounting service (autofs) is disabled (for example, FSTEC of Russia Profile No. 239 for RED OS and ALT Linux), error messages may appear or incorrect scan results may be generated.
- Reports cannot be exported when the number of records is more than 1 million. To resolve this issue, we recommend reducing the number of fields (columns) in a report.
- The solution databases must be available at startup of Kaspersky Vulnerability Management components. Otherwise, the components of the solution cannot start. To solve this issue, you need to wait until the solution database is ready to accept connections and then start the solution components using the `sudo /opt/kaspersky/vulnerability-management/helper/helper.sh start` command.
- While the *Agentless white-box scanning* task is running, the background task service may consume a lot of RAM if the assets being scanned are infected and respond to attempts to connect to them in an excessive way. To reduce the likelihood of exhausting memory, in the task settings, we recommend not including assets that you can scan for vulnerabilities using other types of scans, or increasing the period of the task.
- When you call up Help from sections of Kaspersky Next Vulnerability Management, the start page of the help opens instead of the page relevant to the context.
- The **Vulnerability name**, **Description**, and **Recommendations to fix vulnerabilities** fields are displayed in the language of the Kaspersky Security Center Web Console user interface that was used when creating the report. Changing the UI language does not change the language of these fields.

FIXED ISSUES

The following issues were found in Kaspersky Vulnerability Management version 1.0 and fixed in version 1.0.1:

- Fixed an issue that prevented dragging table lines in the New report template wizard and in the **Data presentation** section of report template properties.
- Fixed an issue that prevented removing entries in the asset card on the **Detected vulnerabilities** tab for vulnerabilities that had been detected using agentless black-box scanning and then fixed and rescanned.

© 2026 AO Kaspersky Lab.