Vulnerability Scanning

Armor Knowledge Base

Topics Discussed

To fully use this screen, you must add the following permissions to your account:

- View Vulnerability Scans
- Write New Vulnerability Report
- View Vulnerability Exclusions
- Write Vulnerability Exclusions

You can use the **Vulnerability Scanning** screen to view scan reports. One report will reflect all of your virtual machines or servers; in these reports, your virtual machines are displayed using their Armor-assigned instance ID.

Scans take place continuously; however, the process to compile a week's worth of data into a single report begins every Sunday at approximately 10:00 PM, Central Standard Time. When a report is complete, it will be available in the **Reports** screen. Based on your data center's location and your environment, your report's availability in AMP may vary.

Vulnerabilities

You can use the **Vulnerabilities** screen to view information for a specific vulnerability scanning report within an interactive table.

This screen also displays a description of the detected vulnerability, including links to external resources, such as the National Vulnerability Database.

You can use this information to prioritize how to troubleshoot these vulnerabilities, as well as understand how these vulnerabilities can affect your environment.

This screen also displays severity levels for each detected vulnerability. A severity is assigned to a vulnerability based on the Common Vulnerability Scoring System (CVSS). CVSS is the accepted system to rate the severity status of a vulnerability. To learn more, please see the National Vulnerability Database website.

Regarding Severity Scoring - Qualys associates each vulnerability with a vulnerability category and most vulnerabilities relate to a generic vulnerability category such as Database or Firewall. These categories all map Severity and CVSS score as described in our documentation. However, there are other vulnerabilities that map to specific platforms and/or vendors (such as Red Hat) and Qualys takes into consideration the context of vendor specific recommendations as they map severity and in these cases, scoring will differ from the Armor's documentation.

For more information, please see Qualys' documentation regarding the Relationship Between Qualys Severity and CVSS Base Scores.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.

Column	Description
Vulnerability Name	This column displays the name of the vulnerability scan report.
Affected Assets	This column displays the number of assets affected by the vulnerability.
Excluded Assets	This column displays the number of assets excluded from the scan for the vulnerability.

CVSS Score	This columns displays the Common Vulnerability Scoring System (CVSS) score assigned to the vulnerability. The breakdown of CVSS Scores aligns with the Severity types.
Severity	This column displays the severity level of the vulnerability. There are four severity types, based on the vulnerability's CVSS: • **Critical** vulnerabilities receive a score of 10. • **High** vulnerabilities receive a score of 7-10. • **Medium** vulnerabilities receive a score of 4-7. • **Low** vulnerabilities receive a score of 0-4. ⚠ There is an additional severity type called **Info**. Although **Info** is listed as a severity type, in reality, **Info** simply displays activity information for corresponding plugins from third-party vendors.
Known Exploits	This column indicates if there are any known exploits for the vulnerability. • **Yes** indicates that a known exploit exists for the vulnerability. • **No** indicates that there are no known exploits.

Exclusions

Vulnerability Exclusions give users the ability to manage their vulnerability programs. Users can exclude vulnerabilities on specific reports or silence them to be addressed later.

Column	Description
Vulnerability	This column displays the name of the vulnerability excluded.
Excluded Assets	This column displays the number of assets excluded from the scan for the vulnerability.
Reason	This column displays the risk reason selected in the Exclude Assets form.
CVSS Score	This columns displays the Common Vulnerability Scoring System (CVSS) score assigned to the vulnerability. The breakdown of CVSS Scores aligns with the Severity types.
Severity	This column displays the severity level of the vulnerability. There are four severity types, based on the vulnerability's CVSS: • **Critical** vulnerabilities receive a score of 10. • **High** vulnerabilities receive a score of 7-10. • **Medium** vulnerabilities receive a score of 4-7. • **Low** vulnerabilities receive a score of 0-4. ⚠ There is an additional severity type called **Info**. Although **Info** is listed as a severity type, in reality, **Info** simply displays activity information for corresponding plugins from third-party vendors.
Known Exploits	This column indicates if there are any known exploits for the vulnerability. • **Yes** indicates that a known exploit exists for the vulnerability. • **No** indicates that there are no known exploits.

Users can filter the table by any of the columns listed above.

Clicking the **Menu** icon to the right of the **Expires On** column allows users to **View** a read-only copy of the Exclusion Details or **Remove Exclusions** from the associated assets.

Reports

The **Reports** screen displays a table of completed reports. Reports are compiled and published on a weekly basis.

Column	Description
Report Name	Reports are named by the date on which they are imported from the VS service.
Import Time	Import time is the time at which the report is imported into AMP.
Import Status	Import status is the status of the report job. Reports listed will show a status of either **Completed** or **InProgress**.
Vulnerabilities	This column provides an at-a-glance view of the number of vulnerabilities included in a specific report, grouped by severity.

Data from within a Report can be filtered either by **Vulnerability** or **Virtual Machine** using the tabs at the top of the report.

View a Report

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.
3. Click the **Reports** tab.
4. Locate and select the desired scan.
5. On the next screen, you can filter the table **By Vulnerabilities** or **By VM** (virtual machine / host).

Troubleshooting

If you do not see any data in the **Vulnerability Scanning** screen, consider that:

- The scanning is not complete.
  - The scan takes place every Sunday at approximately 10:00 PM, local server time.
- You do not have permission to view this screen.
  - You must have the **View Vulnerability Scans** permission enabled. Contact your account administrator to enable this permission. To learn how to update your permissions, see Roles and Permissions.

If a virtual machine is incorrectly labeled as **offline** in a report, then contact Armor Support to run the Armor Toolbox.

Filter By Vulnerabilities

When you filter the table **By Vulnerabilities**, you will see:

COLUMN NAME	DESCRIPTION
Vulnerability Name	This column displays the name of the vulnerability. You can click the **Vulnerability Name** to learn more about the vulnerability. You will be taken to a detailed page where you can review a description of the vulnerability, along with the solution. To learn how to troubleshoot, see Troubleshoot a vulnerability.
Affected Assests	This column displays the virtual machines (host) affected by the vulnerability. If you are unfamiliar with the name of a virtual machine, you can use the **Virtual Machines** screen to search. 1. Copy the desired virtual machine name (host name or CoreInstance ID). 2. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**. 3. Click **Virtual Machines**. 4. In the search field, paste the virtual machine name (host name or CoreInstance ID), and then click the magnifying glass icon.
Category	This column displays the category(s) associated with the vulnerability.
Known Exploits	This column indicates if there are any known exploits for the vulnerability. - **Yes** indicates that a known exploit exists for the vulnerability. - **No** indicates that there are no known exploits.

Severity	This column displays the severity of the vulnerability. There are four severity types, based on the vulnerability's CVSS: • **Critical** vulnerabilities receive a score of 10. • **High** vulnerabilities receive a score of 7-10. • **Medium** vulnerabilities receive a score of 4-7. • **Low** vulnerabilities receive a score of 0-4. There is an additional severity type called **Info**. Although **Info** is listed as a severity type, in reality, **Info** simply displays activity information for corresponding plugins from third-party vendors.

Filter By Virtual Machines

You will only see vulnerabilities for your active virtual machines.

When you filter the table **By VM** (virtual machines / host) you will see:

COLUMN	DESCRIPTION
VM Name	This column displays the virtual machines (host) affected by this vulnerability. If you are unfamiliar with the name of a virtual machine, you can use the **Virtual Machines** screen to search. 1. Copy the desired virtual machine name (host name or CoreInstance ID). 2. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**. 3. Click **Virtual Machines**. 4. In the search field, paste the virtual machine name (host name or CoreInstance ID), and then click the magnifying glass icon.
Last Scan	This column displays the date and time of the last scan.
Critical	This column displays the number of vulnerabilities that contained a score of 10.
High	This column displays a vulnerability that scored between 7 to 10 on the CVSS.
Medium	This column displays a vulnerability that scored between 4 to 7 on the CVSS.
Low	This column displays a vulnerability that scored between 0 to 4 on the CVSS.
Info	This column displays activity information regarding corresponding plugins from a third-party vendor.

Request a New Vulnerability Scan Report

A weekly vulnerability scan report is available in AMP. If you want a new report outside of the weekly report, you can request an "ad-hoc" report once every 24 hours.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.
3. Click the **Reports** tab.
4. Click **Get New Report**.

   ⚠ Requests are limited to once every 24 hours. If a scan report was completed within the last 24 hours, then the **Get New Report** button will be disabled.

5. In the **New Report Request** window, click **Submit**.

   - The latest scan report will be requested, and will display in the list of reports on the **Vulnerability Scanning** screen in a **Pending** status.
   - You may need to refresh the page to view the report status.

⚠ If you recently provisioned a new virtual machine or recently patched a vulnerability, Armor recommends that you wait at least 6 hours to ensure the changes are reflected in the latest report.

Export a Report of Vulnerabilities

From the **By Vulnerability** section, you can also download a CSV report.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.
3. Click **By Vulnerability**.
4. (Optional) Ue the filter function to customize the data displayed.
5. Below the table, click **CSV**.
    - You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Export a Report of a Virtual Machines

From the **By VM** section, you can also download a CSV report.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.
3. Click **By VM**.
4. (Optional) Ue the filter function to customize the data displayed.
5. Below the table, click **CSV**.
    - You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Troubleshooting

Each listed vulnerability contains information on how to troubleshoot the vulnerability, typically by downloading a patch from an external source.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Vulnerability Scanning**.
3. Select a vulnerability scanning report.
4. In the next screen, select **By Vulnerabilities**.
5. Select a vulnerability. You will be taken to a description page where you can review a description of the vulnerability, including the solution.
6. Under **See Also**, click the link to access external information and to download a patch.

⚠ To return to the previous screen and view additional vulnerabilities for the current report, click the name of the current report in the top menu.

Troubleshooting

If you do not see any data in the **Vulnerability Scanning** screen, consider that:

- The scanning is not complete.
    - The scan takes place every Sunday at approximately 10:00 PM, local server time.
- Your firewall rules have not been updated to support this feature.

INBOUND / OUTBOUND	SERVICE / PURPOSE	PORT	DESTINATION
Outbound	Vulnerability Scanning	*443/tcp	64.39.96.0/20 • (qagpublic.qg3.apps.qualys.com)

  * The agent will perform a lookup to the applicable DNS entry, which may resolve to one of multiple Amazon Web Services based subnets. As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.
- You do not have permission to view this screen.
    - You must have the **View Vulnerability Scans** permission enabled. Contact your account administrator to enable this permission. To learn how to update your permissions, see Roles and Permissions.

If a virtual machine is incorrectly labeled as **offline** in a report, then contact Armor Support to run the Armor Toolbox.

Related Documentation

- Vulnerability Scanning for Compliance
- Vulnerability Scanning Exclusions

Was this helpful?

Your Rating:  Results:  14 rates