Platform Performance Improvement FAQ - Info Plugins

What is the background and purpose of the improvement?

Tenable Nessus scanners collect informational (“Info”) data in all default scan configurations. There are over 20,000 different types of Info findings that Nessus scanners can collect. When Nessus scanners are enabled to collect Info data, the Info data can represent more than 90% of all findings per asset, and in the case of port scanning (open ports), Info data accounts for more than 40% of all findings data.

To optimize platform processing performance, Tenable has added a global platform setting - **Relocate Open Port Findings** - that allows you to disable the excessive processing of high-traffic Info plugins. Enabling the setting consolidates the port-related findings of 10 high-traffic plugins. You can then view the consolidated port findings on the **Asset Details** > **Open Ports** tab. The 10 affected plugins are:

- 34220 — Netstat Portscanner (WMI)
- 34252 — Microsoft Windows Remote Listeners Enumeration (WMI)
- 11219 — Nessus SYN Scanner
- 14272 — Netstat Portscanner (SSH)
- 25221 — Remote listeners enumeration (Linux / AIX)
- 99265 — macOS Remote Listeners Enumeration
- 10335 — Nessus TCP scanner
- 14274 — Nessus SNMP Scanner
- 34277 — Nessus UDP Scanner

What are "high-traffic" Info plugins?

In the case of this update, high-traffic plugins are plugins that perform host port scans.

Who is the improvement available to, and when will it be available?

The improvement is now available to all Tenable platform customers. Administrators can configure the improvement by enabling the **Relocate Open Port Findings** setting in the **Settings > General > Scanning** section of Tenable Vulnerability Management.

What are the benefits of the improvement?

By reducing the total number of findings processed substantially, you can expect improved export performance and end-to-end processing times per scan. The magnitude of improvement varies depending on the scale of your deployment, global region, and the breadth of adoption across each region.

Does this change vulnerability detection, reports, and export results?

No. All vulnerability data and features still function as expected. The improvement only impacts a small number of port scanning Info plugins post-scanning.

Where can I find my info port data with this change?

When the optimization is enabled, you can find your Info port data in the **Assets** and **Findings** pages of the Tenable Vulnerability Management user interface. For more information, see the Tenable Vulnerability Management New Data Format: Relocate Open Port Findings whitepaper.

Does this change my PCI scans?

No. Info plugin data is already filtered from the PCI product.

What if I decide not to use this optimization?

In the short term, there are no changes to your environment. However, on a later date, Tenable will permanently restructure the high-traffic findings to optimize their usage and processing performance. Tenable recommends that you use the **Relocate Open Port Findings** optimization to minimize the impact of future restructuring.

Will I see any visual or data differences in the product as a result electing this change?

Yes. Your total finding counts when `Severity = INFO` will decrease. This does not include “vulnerability findings”; this is only includes Info-level data.

How do I know if this impacts me?

The optimization may impact your integrations, reports, and exports if:

- You use the following Info plugin results:
  - 34220 - Netstat Portscanner (WMI)
  - 34252 - Microsoft Windows Remote Listeners Enumeration (WMI)
  - 11219 - Nessus SYN Scanner
  - 14272 - Netstat Portscanner (SSH)
  - 25221 - Remote listeners enumeration (Linux / AIX)
  - 99265 - macOS Remote Listeners Enumeration
  - 10335 - Nessus TCP scanner
  - 14274 - Nessus SNMP Scanner
  - 34277 - Nessus UDP Scanner
- You use the following filter or aggregation criteria:
  - Severity = **INFO**
  - Port

The data in these plugins will not be available to query or export in the Tenable Vulnerability Management user interface or query APIs. However, your raw scan data is still available in the scan DBs. To collect your scan data, follow the instructions in the Collecting Scan Results from Tenable Products community article or use the export-scans API endpoint.

What do I do with old or stale data now that I am not processing these plugins anymore?

Any stale Info-level data on assets and their associated findings will age out after 15 months of not being viewed in the Tenable Vulnerability Management user interface.

What do I need to do to take advantage of the benefits?

Configure whether Tenable Vulnerability Management processes the affected plugins with the **Relocate Open Port Findings** setting. Tenable recommends validating the following checklist to understand the potential impact on your process.

Validation checklist

Before disabling the **Relocate Open Port Findings** setting, validate and acknowledge the following:

- **Report & Widget Results**

  Your total Info findings count will decline substantially, and any port scan results will be removed.

- **Exports**

  Export file size and duration will be reduced.

- **API**

  Queries and custom integrations that filter on or use open port findings for downstream processes will no longer receive data from the affected plugins.

If you do not use port scan Info findings within Tenable products or external processes, Tenable recommends taking advantage of this improvement.

This is not to be confused with port values in vulnerability findings; these values remain intact and are unaffected. To identify the Info findings that will not be processed, use the following filter: `Severity = INFO` and `PluginID = 34220, 34252, 11219, 14272, 99265, 10335, 14274, 34277`.