Tenable Windows Host Data Normalization FAQ

Last Revised: July 27, 2026

Tenable Windows Host Data Normalization FAQ

What is happening?

Tenable is adding a normalization routine to the plugin that collects and reports operating system (OS) information for assessed assets so that Tenable products show more consistent OS results. The plugin will normalize a variety of English-language Windows OS names and versions in credentialed scan results.

Why is this necessary?

Different releases of Windows respond with a variety of information to the queries performed by Tenable Nessus and Tenable Agent during credentialed scans to catalog an asset's OS. The query results occasionally present differently based on the different functions used by Tenable Nessus and Tenable Agent, as well as the specific Windows release and version being scanned.

How does it work?

Tenable products will normalize the various representations of Windows OS names and versions as a standard set of fields:

<vendor> <os> <version> <edition> <update>

How does this update affect me?

Today, if you have Windows assets, they may show up in your Tenable product's asset list with minor variations in the detected OS based on whether a remote scanner or an agent performed the detection. Once the update is released, you will see a normalized OS value for the asset's operating system. For example:

Remote scan – Microsoft Windows 11 Enterprise Build 22621

Agent metadata update – Microsoft Windows 11 Enterprise 10.0.22621 0

Normalized – Microsoft Windows 11 Enterprise Build 22621

Remote scan – Microsoft Windows Server 2019 Datacenter Build 17763

Agent metadata update – Microsoft Windows Server 2019 Datacenter 10.0.17763

Normalized – Microsoft Windows Server 2019 Datacenter Build 17763

Remote scan – Hyper-V Server 2016 Build 14393

Agent metadata update – Hyper-V Server 2016 10.0.14393

Normalized – Microsoft Hyper-V Server 2016 Build 14393

This is just one set of examples; many other Windows OS variations will be updated by this change.

When is Tenable releasing the update?

Tenable products will automatically receive this update on November 8, 2023.

What products does this change affect?

Any Tenable product that uses OS data collected by plugins. This includes:

- Tenable Nessus
- Tenable One Vulnerability Management
- Tenable Security Center

What changes do I need to make?

You do not need to change your Tenable product manually to receive this feature. Your product will update automatically along with the plugin feed.

However, if you have built filters, saved searches, tags, queries, or asset lists that are filtered on expected variations of specific OS values (for example, "Microsoft Windows Server 2019 Datacenter 10.0.17763"), you should update these saved filters.

Moreover, Tenable recommends revisiting any other views that are based on these searches (for example, **Dashboards** or **Reports**) and ensure that they still show data about the expected assets. You only need to revise your searches if they attempt to group assets using the **Operating System** value assigned to them, and you are using a more specific search than a single string (for example, "Windows 11").

Why did Tenable not make this change earlier?

Windows versions began reflecting the specific build number in the last few years, and in that time, customers began to express a concern that this detail was showing up differently based on the conducted scan type. Tenable moved to address this concern and ensured no impact to the products' other asset management features.

Will Tenable release this update for languages besides English or OSs besides Windows?

Yes. As Tenable continues to collect customer feedback, Tenable will incorporate these other use cases into the normalization process. Share feedback with your Tenable Customer Success Manager (CSM) if you have encountered this issue with other operating systems. Tenable will announce future updates via the same communication channels as this update.