Enterprise TruRisk™ Platform

Limited Customer Release Notes

Version 10.35.1

August 21, 2025

What's New?

Vulnerability Management

Enhancement in the Approach to Delete IG

Enhancement in the Approach to Delete IG

When a scan is performed on the agent-installed host, if Information QIDs (IG QIDs) are found, they can be reported only by remote scans (Scanner Specific) and not by the agents. In such cases, agents cannot close or remove the IGs unless they have reported them.

Earlier, when an unauthenticated remote scan was performed, an unauthenticated IG was reported, and it was stored in the database. However, after a few unauthenticated scans, the IG was not reported in subsequent scan results. As per the design, if an IG is not reported in subsequent scans, it must be deleted. But here, the IG was not getting deleted or updated, as an unauthenticated scan was being performed on the host with the agent installed. As a result, the IG remained in the database, which was considered a stale IG.

With this release, we have provided an approach to delete the IGs from the database by satisfying the following specific conditions to ensure proper deletion.

Conditions: You must have performed a remote (Scanner Specific) scan, an unauthenticated scan, and the agent must be installed on that host. You must also have your subscription.

Now, when you perform a scan, and if the above conditions are satisfied, IG will be deleted from the database. If the subscription ID is not your subscription or if an agent supports a QID, the deletion of IG will be skipped, as per the existing behaviour.

With this approach, all stale IG records are deleted automatically, ensuring clean and accurate asset and vulnerability data. You can then take appropriate actions on the detected IGs, saving time and reducing the efforts of manual database cleaning.