Verify VDB Direct Update Paths and Traffic Impact on FMC

Contents

Issue

When running behind on Vulnerability Database (VDB) updates, administrators need to understand whether VDB updates are cumulative and if they can skip intermediate versions.

In this example, the concern is when updating from VDB version 393 to the version 427. Specifically, there is uncertainty about whether multiple upgrade steps are required or if a direct upgrade path is supported. Additionally, concerns arise about potential service interruptions during the VDB update and subsequent policy deployment process.

Environment

- Secure Firewall Management Center (FMC) software version 7.4.2.4. Other software versions are also affected.
- Firewall Threat Defense (FTD) on FPR 2110. Other hardware platforms are also affected.
- Current VDB version: 393. Other software versions are also affected.
- Target VDB version: 427. Other software versions are also affected.

Resolution

VDB updates on FMC are cumulative, allowing direct upgrades from older versions to newer versions without requiring intermediate steps.

VDB Update Process

You can update directly from VDB version 393 to VDB version 427 without any intermediate VDB upgrade steps. Starting with VDB version 357, Cisco supports installing any VDB version as far back as the baseline VDB on the FMC platform.

To download the latest VDB version, see Software Download.

Service Impact Considerations

The primary risk is not associated with the VDB installation itself on the FMC, but rather with the first policy deployment on FTD after the VDB update. In most cases, the first deployment after a VDB update restarts the Snort process, which interrupts traffic inspection temporarily.

During this interruption period:

- Traffic can either drop or pass without further inspection.
- The specific behavior depends on how the FTD is configured to handle traffic during process restarts.

Best practice recommendations:

- Schedule the policy deployment portion during a planned maintenance window.
- Coordinate with network operations to minimize user impact.
- Monitor system status during and after the deployment process.

Cause

- Starting with VDB 357, you can install any VDB updates as far back as the baseline VDB for the FMC.
- The installation requires a policy redeployment to activate the new vulnerability signatures, which triggers a Snort process restart on managed FTD devices. This restart creates a brief interruption in traffic inspection capabilities while the new database is loaded and the inspection engine reinitializes.

Related Content

- Cisco Secure Firewall Management Center Administration Guide - System Updates
- Cisco Secure Firewall Management Center Device Configuration Guide - Deployment
- Cisco Technical Support & Downloads