Implement Rollback VDB Version in FMC Version 7.3+

Contents

Introduction Prerequisites Requirements Components Used Configure Initial Configurations Rollback Process Verify Limitations Related Information

Introduction

This document describes the process to downgrade the Vulnerability Database on Secure Firewall Management Center (FMC) version 7.3 and later.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

• Cisco Secure Firewall Management Center version 7.3 VDB 361

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Initial Configurations

On the FMC GUI, the VDB version is obtained under the MainMenu > ? > About.

| w | Analysis | Policies | Devices | Objects | Integration | Deploy | Q | 6 | ≎ | 0 | idmin v | | | |
|-----------------|--------------|---------------|---------|-----------------------|----------------|--------|---|---|-------|--------|----------------------|--|--|--|
| Г | About | | | Tools | Tools | | | | | | On-screen Assistance | | | |
| | | | | Firep | ower Migration | Tool | | | Pag | ge-lev | el Help | | | |
| Product Content | | | Appl | Application Detectors | | | | | w-Tos | New | | | | |
| | Sacura Eirau | vall on Cierr | noom | | | | | | | | | | | |

| cisco SECU | RE |
|--|---|
| Firewall M | anagement Center |
| Version 7.3.0 (build 69) Model Serial Number Snort Version Snort3 Version Rule Pack Version Module Pack Version LSP Version | Secure Firewall Management Center for VMware None 2.9.21 (Build 105) 3.1.36.1 (Build 101) 2868 3244 Isp-rel-20230712-1621 build 261 (2022, 11, 15, 10:57:46) |
| Rule Update Version | 2023-07-12-002-vrt |
| Geolocation Update Versi OS | on Country Code: 2023-06-17-100, IP: 2023-06-17-100 Cisco Firepower Extensible Operating System (FX-OS) 2.13.0 (build 198) |
| Hostname | firepower |
| For technical/system question 7209. Copyright 2004-2022, | ns, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526- Cisco and/or its affiliates. All rights reserved. |
| Сору | Close |

On the CLI, the VDB version is obtained with command show version .

<#root>

```
> show version
```

------ [firepower]------Model : Secure Firewall Management Center for VMware (66) Version 7.3.0 (Build 69) UUID : e8f4b5de-4da1-11ed-b2ce-4637a3ef82f7 Rules update version : 2023-07-12-002-vrt LSP version : lsp-rel-20230712-1621

VDB version : 361

Rollback Process

If the previous VDB version is no longer stored on the FMC, navigate to **System** (*) > **Updates** > **Product Updates** > **Available Updates** > **Upload Updates**, select the VDB File from your local computer and click on Upload.

Once the VDB file is uploaded on the FMC, the older VDB version (version 359 in this case) displays a newRollback icon instead of the **Install** icon.

Click on the rollback button.

| | Firewall Management Center System / Updates / Product Updates | Overview | Analysis | Policies | Devices | Objects | Integration |
|---|--|-----------------------------------|----------|----------|---------|-------------|-------------------|
| | Product Updates Rule Updates Geolocation I | Updates | | | | | |
| e | Currently running software version: 7.3.0 Currently installed VDB version: build 361 (2022-11-15 Available Updates Readiness History Downle | 19:57:46) load updates | | | | | |
| | Туре | Version | | | | Date | |
| | Cisco Vulnerability And Fingerprint Database Updates | 361 | | | | Tue Nov 15 | 19:59:36 UTC 2022 |
| | Cisco Vulnerability And Fingerprint Database Updates | 359 | | | | Tue Oct 4 1 | 9:46:46 UTC 2022 |
| | | | | | | | |

Then, check the FMC checkbox and click on Install.

| Product Updates | Rule Updates | Geolocation Updates | | | | | |
|------------------------|---|---------------------------------|----------------|-----------------|------|-------------------------|-------------|
| Currently running soft | ware version: 7.3.0 |) | | | | | |
| Selected Updat | e Type Cisco V Version 359 Date Tue Oct Reboot No | ulnerability And Fingerprint Da | tabase Updates | | | | |
| Ungrouped | (1 total) | | (| Compatibility C | heck | Readiness Check Results | Readiness C |
| hrepower | cure Firewall Manage | ment Center for VMware v7.3.0 | | N/A | | | |

A warning prompt is displayed to inform you about potential traffic disruption in case you deploy changes to the managed Firewalls after the VDB rollback.



Verify

Once the rollback task is completed, the VDB version can be confirmed under the main **Menu** > ② > **About.**

| | × |
|------------------------------|---|
| ululu SECU | DE |
| cisco SECO | KL |
| Firewall M | lanagement Center |
| i ii civaii iv | anagement conter |
| Version 7.3.0 (build 69) | |
| Model | Secure Firewall Management Center for VMware |
| Serial Number | None |
| Snort Version | 2.9.21 (Build 105) |
| Snort3 Version | 3.1.36.1 (Build 101) |
| Rule Pack Version | 2868 |
| Module Pack Version | 3244 |
| LSP Version | lsp-rel-20230712-1621 |
| VDB Version | build 359 (2022-10-04 19:44:54) |
| Rule Update Version | 2023-07-12-002-vrt |
| Geolocation Update Vers | sion Country Code: 2023-06-17-100, IP: 2023-06-17-100 |
| OS | Cisco Firepower Extensible Operating System (FX-OS) |
| | 2.13.0 (build 198) |
| Hostname | firepower |
| For technical/system questic | ons email tac@cisco.com phone: 1-800-553-2447 or 1-408-526- |
| 7209. Copyright 2004-2022 | Cisco and/or its affiliates. All rights reserved. |

Finally, after the VDB is rolled back, a policy deployment is required to push the new VDB configuration to the FMC managed Firewalls.

| * | 0 | FTD-Cluster | System | | FTD | A-1 | Jul 19, 2023 7:00 PM | 8 | Ready for Deployment |
|--------------|---|---|--------|----------|-----|-----|----------------------|---|----------------------|
| :: • 1 | | Access Control Group Access Control Policy: Blank Security Updates VDB: (Build 359 - 2022-10-04 19:44) | :54) | ⊥ System | | | | | |

Limitations

- The VDB rollback button is not available prior FMC 7.3.
- You are unable to rollback the VDB to a version older than 357, if a VDB version older than 357 is uploaded to the FMC, the rollback button is grayed out.

| Cisco Vulnerability And Fingerprint Database Updates | 354 | Wed Apr 27 19:42:09 UTC 2022 | No | 0 | |
|---|-----|------------------------------|----|---|--|
| | | | | VDB rollback is only supported starting with VDB version 35 | |

• If the VDB version is lower than the base VDB version of the FMC, the successful rollback task that is completed is displayed, however, the VDB version displayed continue showing the same as prior the rollback attempt.



From the FMC CLI you can confirm that this happened because the rollback target version is lower than the base FMC version. This can be confirmed on the FMC CLI on the status.log file.

sudo su cd /var/log/sf/vdb-4.5.0-<vdb number>/ cat status.log root@firepower:/var/log/sf/vdb-4.5.0-357# cat status.log state:running ui:The install has begun. ui:[0%] Running script pre/000_start.sh... ui:[0%] Running script pre/010_check_versions.sh... ui:[4%] Running script pre/010_check_versions.sh... ui:[4%] Non-Fatal error: Non-Fatal error: Cannot rollback to version(357) lower than default VDB 358 ui:[4%] The install completed successfully. ui:The install has completed. state:finished

Related Information

<u>Cisco Technical Support & Downloads</u>