Verduidelijking van het proces voor VDB-updates op FMC

Inhoud

uitgifte

Wanneer beheerders achterlopen op VDB-updates (Vulnerability Database), moeten ze begrijpen of VDB-updates cumulatief zijn en of ze tussenliggende versies kunnen overslaan.

In dit voorbeeld is het probleem bij het updaten van VDB-versie 393 naar versie 427. Er is met name onzekerheid over de vraag of meerdere upgradestappen vereist zijn of dat een direct upgradepad wordt ondersteund. Daarnaast zijn er zorgen over mogelijke onderbrekingen van de service tijdens de VDB-update en het daaropvolgende beleidsimplementatieproces.

milieu

- Secure Firewall Management Center (FMC) softwareversie 7.4.2.4. Ook andere softwareversies worden getroffen.
- Firewall Threat Defense (FTD) op FPR 2110. Ook andere hardwareplatforms worden getroffen.
- Huidige VDB-versie: 393. Ook andere softwareversies worden getroffen.
- Doelversie VDB: 427. Ook andere softwareversies worden getroffen.

resolutie

VDB-updates op FMC zijn cumulatief, waardoor directe upgrades van oudere versies naar nieuwere versies mogelijk zijn zonder tussenstappen.

VDB-updateproces

U kunt rechtstreeks van VDB-versie 393 naar VDB-versie 427 updaten zonder tussenliggende VDB-upgradestappen. Vanaf VDB versie 357 ondersteunt Cisco het installeren van elke VDB versie zo ver terug als de basislijn VDB op het FMC platform.

Als u de nieuwste VDB-versie wilt downloaden, gaat u naar het Cisco Software Download Center op https://software.cisco.com/download/home/286332319/type/286321931/release/VDB

Overwegingen met betrekking tot de impact op de dienstverlening

Het primaire risico houdt geen verband met de VDB-installatie zelf op het FMC, maar eerder met de eerste beleidsimplementatie op FTD na de VDB-update. In de meeste gevallen start de eerste implementatie na een VDB-update het Snort-proces opnieuw, waardoor de verkeersinspectie tijdelijk wordt onderbroken.

Tijdens deze onderbrekingsperiode:

- Het verkeer kan zonder verdere inspectie dalen of passeren.
- Het specifieke gedrag hangt af van de manier waarop de FTD is geconfigureerd om verkeer te verwerken tijdens het opnieuw opstarten van het proces.

Aanbevelingen voor beste praktijken:

- Plan de beleidsimplementatie tijdens een gepland onderhoudsvenster.
- Coördineren met netwerkactiviteiten om de impact van de gebruiker te minimaliseren.
- Controleer de systeemstatus tijdens en na het implementatieproces.

Oorzaak

- Vanaf VDB 357 kunt u alle VDB-updates installeren tot de basislijn VDB voor de FMC.

- De installatie vereist een beleidsherimplementatie om de nieuwe kwetsbaarheidshandtekeningen te activeren, waardoor een Snort-proces opnieuw wordt opgestart op beheerde FTD-apparaten. Deze herstart zorgt voor een korte onderbreking van de verkeersinspectiemogelijkheden terwijl de nieuwe database wordt geladen en de inspectiemotor opnieuw wordt geïnitialiseerd.

Gerelateerde inhoud

- Beheergids voor Cisco Secure Firewall Management Center - Systeemupdates
- Configuratiehandleiding voor Cisco Secure Firewall Management Center-apparaten - Implementatie
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.