Klärung des VDB-Aktualisierungsprozesses auf FMC

Inhalt

Problem

Wenn VDB-Updates (Vulnerability Database) im Hintergrund ausgeführt werden, müssen Administratoren wissen, ob VDB-Updates kumulativ sind und ob sie Zwischenversionen überspringen können.

In diesem Beispiel ist die Aktualisierung von VDB-Version 393 auf Version 427 problematisch. Insbesondere besteht Unsicherheit darüber, ob mehrere Upgrade-Schritte erforderlich sind oder ob ein direkter Upgrade-Pfad unterstützt wird. Darüber hinaus bestehen Bedenken hinsichtlich möglicher Service-Unterbrechungen während des VDB-Updates und des anschließenden Prozesses der Richtlinienbereitstellung.

Umwelt

- Secure Firewall Management Center (FMC) Softwareversion 7.4.2.4. Andere Softwareversionen sind ebenfalls betroffen.
- Firewall Threat Defense (FTD) auf FPR 2110. Auch andere Hardwareplattformen sind betroffen.
- Aktuelle VDB-Version: 393. Andere Softwareversionen sind ebenfalls betroffen.
- VDB-Zielversion: 427. Andere Softwareversionen sind ebenfalls betroffen.

Auflösung

VDB-Updates auf FMC sind kumulativ und ermöglichen direkte Upgrades von älteren auf neuere

Versionen ohne Zwischenschritte.

VDB-Aktualisierungsprozess

Sie können direkt von VDB-Version 393 auf VDB-Version 427 aktualisieren, ohne Zwischenschritte für ein VDB-Upgrade durchzuführen. Ab VDB-Version 357 unterstützt Cisco die Installation jeder VDB-Version bis zurück zur Basis-VDB auf der FMC-Plattform.

Um die neueste VDB-Version herunterzuladen, navigieren Sie zum Cisco Software Download Center unter https://software.cisco.com/download/home/286332319/type/286321931/release/VDB

Überlegungen zu den Auswirkungen auf Services

Das Hauptrisiko ist nicht mit der VDB-Installation selbst auf dem FMC verbunden, sondern mit der ersten Richtlinienbereitstellung auf FTD nach dem VDB-Update. In den meisten Fällen wird der Snort-Prozess bei der ersten Bereitstellung nach einem VDB-Update neu gestartet, wodurch die Datenverkehrsanalyse vorübergehend unterbrochen wird.

Während dieser Unterbrechungszeit:

- Der Datenverkehr kann ohne weitere Überprüfung entweder unterbrochen oder unterbrochen werden.
- Das genaue Verhalten hängt davon ab, wie die FTD konfiguriert ist, um Datenverkehr während Prozessneustarts zu verarbeiten.

Empfehlungen zu Best Practices:

- Planen Sie die Bereitstellung der Richtlinie während eines geplanten Wartungsfensters.
- Koordination mit dem Netzwerkbetrieb zur Minimierung der Auswirkungen auf die Benutzer
- Überwachung des Systemstatus während und nach der Bereitstellung

Ursache

- Ab VDB 357 können Sie beliebige VDB-Updates bis zurück zur Basis-VDB für das FMC installieren.
- Die Installation erfordert eine Neubereitstellung der Richtlinien, um die neuen Schwachstellensignaturen zu aktivieren. Dies löst einen Neustart des Snort-Prozesses auf verwalteten FTD-Geräten aus. Dieser Neustart führt zu einer kurzen Unterbrechung der Datenverkehrsanalyse, während die neue Datenbank geladen wird und die Prüfungs-Engine neu initialisiert wird.

Verwandte Inhalte

- Administrationsleitfaden für Cisco Secure Firewall Management Center - System-Updates
- Konfigurationsleitfaden für Cisco Secure Firewall Management Center-Geräte - Bereitstellung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.