Problemen met FMC-indringers oplossen die impact=onbekend aantonen

Inhoud

uitgeven

Na de implementatie van een nieuw Firewall Management Center (FMC) en de upgrade naar versie 7.7.12, worden alle inbraakgebeurtenissen weergegeven met "Impact=Unknown" in plaats van de verwachte impactwaarden. Dit voorkomt dat de juiste waarschuwingsmechanismen worden geactiveerd, omdat het impactveld nodig is voor de waarschuwingsconfiguratie.

milieu

- FMC versie 7.7.12. Ook andere softwareversies kunnen worden beïnvloed.
- Inbraakbeleid in de preventie- of detectiemodus.

resolutie

De oplossing voor dit probleem bestaat uit het verifiëren en configureren van de reikwijdte van het detectiebeleid zodat alle relevante IP-adressen worden opgenomen waarop inbraakgebeurtenissen worden gegenereerd.

Stap 1. Betrokken IP-adressen identificeren

Controleer de inbraakgebeurtenissen die "Impact=Unknown" tonen en identificeer de specifieke IP-adressen die bij deze gebeurtenissen betrokken zijn. Documenteer deze IP-adressen voor

vergelijking met de huidige configuratie van het detectiebeleid.

Stap 2. De huidige configuratie van het opsporingsbeleid bekijken

Navigeer naar FMC Policies > Network Discovery (in nieuwere versies is dit Policies > Advanced > Network Discovery) en bekijk de huidige instellingen voor het detectiebeleid om te bepalen welke IP-adresbereiken of subnetten momenteel in het detectiebereik zijn opgenomen.

Stap 3. Bereik opsporingsbeleid bijwerken

Wijzig de configuratie van het opsporingsbeleid om alle IP-adressen op te nemen waar zich inbraakgebeurtenissen voordoen. Zorg ervoor dat de reikwijdte van het detectiebeleid alle netwerksegmenten omvat waar u verwacht inbraakgebeurtenissen te ontvangen met de juiste effectbeoordeling.

Stap 4. Configuratiewijzigingen implementeren

Implementeer de bijgewerkte configuratie van het opsporingsbeleid op alle beheerde apparaten om ervoor te zorgen dat de wijzigingen in de gehele beveiligingsinfrastructuur worden doorgevoerd.

Stap 5. Impact-veldpopulatie controleren

Controleer nieuwe inbraakgebeurtenissen om te bevestigen dat het impactveld nu wordt gevuld met de juiste waarden in plaats van "Onbekend".

Oorzaak

De indringingsgebeurtenissen die "Impact=Unknown" lieten zien, werden veroorzaakt door een configuratieprobleem waarbij de betreffende IP-adressen niet waren opgenomen in een detectiebeleid op de FMC. Wanneer IP-adressen buiten het bereik van geconfigureerde detectiebeleidsregels vallen, kan de FMC de impact van inbraakgebeurtenissen voor die adressen niet goed beoordelen, waardoor het impactveld wordt gevuld met "Onbekende" waarden. Dit is een probleem met de configuratie in plaats van een software- of hardwarefout.

Verwante inhoud

- Intrusion Event Impact Levels
- 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.