# Fehlerbehebung bei FMC-Angriffsereignissen mit Auswirkungen = unbekannt

## Inhalt

## Problem

Nach der Bereitstellung eines neuen Firewall Management Center (FMC) und dem Upgrade auf Version 7.7.12 zeigen alle Angriffsversuche "Impact=Unknown" anstelle der erwarteten Auswirkungswerte an. Dadurch wird verhindert, dass geeignete Warnmechanismen ausgelöst werden, da das Auswirkungsfeld für die Warnkonfiguration erforderlich ist.

## Umwelt

- FMC Version 7.7.12. Andere Softwareversionen können ebenfalls betroffen sein.
- Angriffsrichtlinie im Präventions- oder Erkennungsmodus.

## Auflösung

Zur Lösung dieses Problems muss der Bereich der Erkennungsrichtlinie überprüft und so konfiguriert werden, dass er alle relevanten IP-Adressen enthält, an denen Angriffsereignisse generiert werden.

### Schritt 1: Identifizieren der betroffenen IP-Adressen

Überprüfen Sie die Angriffsversuche, bei denen "Impact=Unknown" angezeigt wird, und identifizieren Sie die spezifischen IP-Adressen, die an diesen Ereignissen beteiligt sind.

Dokumentieren Sie diese IP-Adressen für einen Vergleich mit der aktuellen Discovery Policy-Konfiguration.

## Schritt 2: Überprüfen der aktuellen Discovery Policy-Konfiguration

Navigieren Sie zu FMC Policies > Network Discovery (in neueren Versionen ist Policies > Advanced > Network Discovery), und überprüfen Sie die aktuellen Einstellungen der Erkennungsrichtlinie, um zu bestimmen, welche IP-Adressbereiche oder Subnetze derzeit im Erkennungsbereich enthalten sind.

## Schritt 3: Erkundungsrichtlinienbereich aktualisieren

Ändern Sie die Konfiguration der Erkennungsrichtlinie, um alle IP-Adressen einzuschließen, an denen Angriffsereignisse auftreten. Stellen Sie sicher, dass der Geltungsbereich der Erkennungsrichtlinie alle Netzwerksegmente umfasst, in denen Sie Angriffsversuche erwarten, und zwar mit einer ordnungsgemäßen Auswirkungsanalyse.

## Schritt 4: Bereitstellen von Konfigurationsänderungen

Stellen Sie die aktualisierte Discovery Policy-Konfiguration auf allen verwalteten Geräten bereit, um sicherzustellen, dass die Änderungen in der gesamten Sicherheitsinfrastruktur wirksam werden.

## Schritt 5: Auswirkungsfeldauffüllung überprüfen

Überwachen Sie neue Angriffsereignisse, um sicherzustellen, dass das Auswirkungsfeld jetzt mit den entsprechenden Werten anstatt "Unbekannt" gefüllt wird.

## Ursache

Die "Impact=Unknown" anzeigenden Angriffsereignisse wurden durch ein Konfigurationsproblem verursacht, bei dem die betroffenen IP-Adressen nicht in einer Erkennungsrichtlinie auf dem FMC enthalten waren. Wenn IP-Adressen nicht in den Geltungsbereich der konfigurierten Erkennungsrichtlinien fallen, kann das FMC die Auswirkungen von Angriffsversuchen für diese Adressen nicht ordnungsgemäß bewerten, sodass im Feld "Auswirkungen" die Werte "Unbekannt" eingetragen werden. Dies ist eher ein Problem mit der Konfiguration als ein Software- oder Hardwarefehler.

## Verwandte Inhalte

- Auswirkungsstufen von Angriffen
- 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.