FMC Unified Events-Suche schlägt fehl bei Netzwerkobjektnamen in FirePOWER 7.7

Problem

Bei Verwendung von Cisco Secure Firewall Management Center (FMC) Version 7.7.10.1 können Netzwerkobjekte und Objektgruppen nicht als Suchkriterien auf der Seite "Unified Events" verwendet werden. Bei dem Versuch, in der Unified Event-Suche unter Quell-IP nach Ereignissen mit bestimmten Objekt- oder Gruppennamen zu suchen, gibt das FMC entweder keine Ergebnisse zurück oder zeigt eine Fehlermeldung an:

```
The query contains an invalid constraint on the provided field: "Source IP" with value "${000_ALL-USER_
```

Die Objekte sind sichtbar und können unter Objektverwaltung verwendet werden, und die Suche nach Roh-IP-Adresse funktioniert wie erwartet. Dieses Verhalten wirkt sich sowohl auf vorhandene als auch auf neu erstellte Netzwerkobjekte aus, wodurch die Suche nach Ereignissen mithilfe von Objekt- oder Gruppennamen in der Unified Events-Schnittstelle erschwert wird.

Umwelt

- Cisco Secure Firewall Management Center für VMware (FMCv)
- Software-Version: 7.7.10.1
- Technologie: Cisco Secure Firewall FirePOWER 7.7
- Sub-Technologie: Cisco Secure Firewall - Überwachung/Eventing/Protokollierung - 7.7
- Bereitstellung: Standalone-FMC-Konfiguration
- FMC enthält über 1000 Netzwerkobjekte
- Umgebung umfasst Migrationshistorie von standortbasiertem FMC zu cdFMC und zurück zu standortbasiertem

Auflösung

Dieses Problem wird durch einen bekannten Softwarefehler verursacht und kann durch Konfigurationsänderungen an der aktuellen Softwareversion nicht vollständig behoben werden. Es wird empfohlen, diesen Auflösungsansatz zu implementieren.

Sofortige Lösung

Verwenden Sie IP-Adressfelder in Unified Event-Suchvorgängen anstelle von Objektnamen oder Gruppen als Zwischenumgehung. Bei der Untersuchung von Ereignissen, die sich auf betroffene Objekte oder Gruppen beziehen:

1. Navigieren Sie zu Analyse > Vereinheitlichte Ereignisse.
2. Verwenden Sie bei den Suchkriterien die tatsächlichen IP-Adressen anstelle von Objektnamen.
3. Geben Sie die spezifische IP-Adresse oder den IP-Bereich in die Felder Quell-IP oder Ziel-IP ein.
4. Führen Sie die Suche aus, um die gewünschten Ereignisse abzurufen.

Langfristige Lösung

Für die dauerhafte Behebung des Problems ist ein Upgrade auf eine zukünftige FMC-Softwareversion erforderlich, die die Auflösung für Cisco Bug-ID CSCws52418 enthält. Gehen Sie wie folgt vor:

1. Abonnieren Sie die Benachrichtigungen über defekte CSCws52418, um Warnmeldungen zu erhalten, wenn feste FMC-Versionen verfügbar werden.
2. Überwachen Sie den Bug-Status, um Updates zur Fix-Verfügbarkeit zu erhalten, die voraussichtlich im Mai 2026 verfügbar sein wird.
3. Planen Sie ein Wartungsfenster, um FMC und verwaltete Geräte auf eine Version zu aktualisieren, die den Fix für CSCws52418 enthält, sobald er veröffentlicht ist.

Prävention und Empfehlungen

Bis zum Abschluss des Software-Upgrades:

- Verwenden Sie IP-basierte Suchkriterien in Unified Events (Quell-/Ziel-IP), wenn Sie Ereignisse in Bezug auf betroffene Objekte oder Gruppen untersuchen.
- Verlassen Sie sich beim Erstellen neuer betrieblicher Workflows nicht ausschließlich auf die Objektnamensuche in Unified Events für Betriebs- oder Überwachungsprozesse in dieser Version.
- Dokumentieren Sie die betroffenen Objektnamen und die zugehörigen IP-Adressen, um sie bei der Fehlerbehebung als Referenz zu verwenden.

Ursache

Das Verhalten wird durch die Cisco Bug-ID CSCws52418 verursacht, bei der die interne Behandlung von Objektsuchvorgängen für Ereignissuchen durch einen internen Grenzwert von ca. 1000 Objekteinträgen eingeschränkt ist. Objekte außerhalb dieses Limits werden bei Unified Event-Suchen nach Namen nicht richtig indiziert oder zurückgegeben, was zu Fehlern bei den Ergebnissen oder "Invalid Constraint"-Fehlern führt. Die Wiederherstellung der monetdb-Ereignisdatenbank löst dieses Verhalten nicht, da es sich um eine codierte Softwarebeschränkung und nicht um ein Datenbankbeschädigungsproblem handelt.

Verwandte Inhalte

- Cisco Bug-ID CSCws52418 - Einige Objekte in den Ereignissuchfiltern nicht zur Auswahl verfügbar
- Cisco Bug-ID CSCwt05296 - Das neu erstellte oder vom System definierte Objekt IPv4-Private-All-RFC1918 kann nicht als Filter für Ereignisse verwendet werden.
- 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.