Snort Engine-Upgrade während FTD-Upgrade aufgrund von Erkennung benutzerdefinierter Richtlinien blockiert

Inhalt

Problem

Während eines FTD-Upgrades von Version 7.2 auf 7.4.4 auf einem HA FPR-4115, das von FMC verwaltet wird, wird das Snort-Engine-Upgrade auf Snort 3 mit Fehlermeldungen blockiert, die darauf hinweisen, dass die benutzerdefinierten Snort 2-Regeln oder die Verwendung benutzerdefinierter Intrusion- oder Netzwerkanalyserichtlinien nicht konvertiert wurden. Die entsprechende Fehlermeldung lautet: "Es kann kein Upgrade auf Snort 3 durchgeführt werden. Das Gerät verwendet mindestens eine benutzerdefinierte Richtlinie für Sicherheitsrisiken oder eine Netzwerkanalyserichtlinie." Eine detailliertere Fehlermeldung verweist auf die Unfähigkeit, benutzerdefinierte Snort 2-Regeln zu konvertieren, und zeigt für weitere Details auf /var/sf/htdocs/ips/snort.rej. Es stellt sich die Frage, ob dieser Fehler die Migration zu Snort 3 verhindern und sich auf die Prüfungsfunktionen auswirken würde.

Umwelt

- Cisco Secure Firewall FirePOWER 7.3
- Firepower Management Center (FMC) Version 7.7.11
- FTD-Geräte in Hochverfügbarkeitskonfiguration
- Hardware: FPR-4115
- Upgrade-Pfad: FTD 7.2 bis 7.4.4
- VDB in der neuesten Version vor dem Upgrade
- Abschnitt "Lokale Regeln" unter "Objekte" > "Angriffsregeln" > "Snort 2" Alle Regeln sind leer.

Auflösung

Die Fehlermeldung, die das Snort-Modul-Upgrade blockiert, ist ein dokumentiertes Verhalten im Zusammenhang mit der Cisco Bug-ID CSCwn46794 und stellt keinen funktionalen Blocker dar, wenn keine benutzerdefinierten Snort 2-Regeln vorhanden sind.

Verifizierungsschritte

Schritt 1: Überprüfen des benutzerdefinierten Snort 2-Regelstatus

Navigieren Sie zur FMC-Schnittstelle, und überprüfen Sie, ob benutzerdefinierte Snort 2-Regeln vorhanden sind:

```
Objekte > Angriffsregeln > Snort 2 Alle Regeln > Lokale Regeln
```

Schritt 2: VDB-Version bestätigen

Stellen Sie sicher, dass die Vulnerability Database (VDB) auf der neuesten Version ist, bevor Sie mit dem Upgrade fortfahren.

Schritt 3: Überprüfen von Fehlerdetails

Überprüfen Sie die detaillierten Fehlerinformationen in der referenzierten Datei:

```
/var/sf/htdocs/ips/snort.rej
```

Upgrade-Prozess

Wenn der Abschnitt "Lokale Regeln" als leer bestätigt wird (keine benutzerdefinierten Snort 2-Regeln vorhanden), kann das Upgrade trotz der Fehlermeldung fortgesetzt werden. Der Blockierungsfehler ist in diesem Szenario falsch positiv und gibt keine tatsächlichen benutzerdefinierten Regeln an, die konvertiert werden müssen.

Schritt 1: Fortsetzen des Snort 3-Upgrades

Fahren Sie mit dem FTD-Upgrade auf Version 7.4.4 fort, das das Upgrade der Snort 3-Engine umfasst.

Schritt 2: Validierung nach dem Upgrade

Nachdem das Upgrade erfolgreich abgeschlossen wurde, testen Sie den Datenverkehrsfluss, um das erwartete Verhalten mit der Snort 3-Engine zu bestätigen.

Schritt 3: Überwachen der Systemleistung

Validieren Sie, dass die Inspektionsfunktion wie erwartet mit der neuen Snort 3 Engine funktioniert.

Ursache

Die Aktualisierungsblockierungsmeldung ist ein dokumentiertes Verhalten, das mit der Cisco Bug-ID CSCwn46794 verknüpft ist. Dieser Fehler bewirkt, dass das System eine Fehlermeldung über benutzerdefinierte Angriffsrichtlinien oder Netzwerkanalyserichtlinien anzeigt, auch wenn keine benutzerdefinierten Snort 2-Regeln vorhanden sind, die eine Konvertierung erfordern. Die Fehlermeldung wird als falsch angezeigt, wenn der Abschnitt "Lokale Regeln" leer ist, die Überprüfung vor dem Upgrade des Systems jedoch das Vorhandensein benutzerdefinierter

Richtlinien falsch identifiziert.

Verwandte Inhalte

- Cisco Bug-ID CSCwn46794
- Cisco Bug-ID CSCwk07199
- 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.