Auswirkungen der Layer-7-Inspektion auf den Multilayer-Datenverkehr: Überprüfung der Snort3-Implementierung

Inhalt

Problem

Nach der Aktivierung der DNS-Sinkhole-Regeln in einer Zugriffskontrollrichtlinie (Access Control Policy, ACP) wurde der gekapselte VXLAN-Datenverkehr unerwartet auf Firepower Threat Defense (FTD)-Geräten mit Snort 3-Modulversionen verworfen.

- VXLAN-gekapselter Datenverkehr bricht nach Aktivierung der DNS Sinkhole Policy ab.
- Verbindungsereignisse mit inneren IP-Adressen (z. B. 100.70.x.x) anstelle von äußeren VXLAN-Headern
- Unerwartetes Verhalten bei der Snort 3-Implementierung während des Labortests.

Umwelt

•Plattform: Hochverfügbarkeitspaar mit FTD

- Betroffene Version: 7.6.2.1 (Snort 3)
- Feste Version: Über 7,6,4 (Snort 3)

Auflösung

Lösung unter 7.6.2.1:

##########

Schritt 1:

Vorfilterrichtlinie (empfohlen)

Erstellen Sie eine Vorfilterregel, um die Snort-Überprüfung für VXLAN-Datenverkehr zu umgehen:

- Vorfilterrichtlinie

•Aktion: FastPath (Tunnelregel)

- Quelle: <Äußerer VXLAN_Source_IPs>

•Ziel: <Outer_VXLAN_Destination_IPs>

•Protokolle: UDP

•Anschluss: 4789

Phase 2:

Vorhandene Verbindungen löschen

- Verbindungsadresse <outer_ip_1> Adresse <outer_ip_2> löschen

Regelreihenfolge anpassen, wenn Vorfilterrichtlinie nicht verwendet wird

Legen Sie L7-Regeln (DNS Sinkhole, App-ID) vor die internen IP-Genehmigungsregeln in ACP.

Langfristige Lösung:

##########

1. Upgrade auf FTD 7.6.4 oder spätere Version

- Löst CSCwo54753 (PSIRT DEFECT)

- Bietet konsistentes mehrschichtiges Prüfverhalten.

2. Konfigurieren Sie interne und externe Regeln für DNS Sinkhole:

- Bei Verwendung von DNS Sinkhole oder anderen Sicherheitsfunktionen mit gekapseltem Datenverkehr.

3. Für Nicht-SI-Layer-7-Funktionen (URL-Filterung, Anwendungskontrolle):

- In ACP sind nur interne Header-Regeln erforderlich.

- Äußere Header-Regeln sind nicht erforderlich.

Weitere Details zur Multi-Layer VXLAN Inspection-Funktion

##

FTD umfasst eine Multi-Layer-Prüfungsfunktion für Security Intelligence (SI) und Layer-7-Funktionen. Diese Funktion bestimmt, ob Snort äußere Kapselungsheader oder innere Payload-Header auf Basis konfigurierter Layer-7-Richtlinien überprüft.

Zu den Layer-7-Funktionen gehören:

DNS Sinkhole

- Anwendungskontrolle (App-ID)

- URL-Filterung

- Geolokalisierung

- Schutz vor Sicherheitsrisiken

Hauptverhalten:

##########

Wenn im ACP irgendeine Layer-7-Funktion aktiviert ist, wird Snort die innersten Header gekapselter Pakete überprüfen (z. B. VXLAN, GRE, IP-in-IP).

Technische Analyse:
##############
Snort 3 (7.6.2.1) - Fehlerhaftes Verhalten

Ohne Layer-7-Regeln:

- Snort basiert auf Verbindungsmetadaten von Lina (ASA-Datenpfad-Engine).
- Datenverkehr wird nur auf Basis von Regeln für äußere Header zugelassen/abgelehnt.
- Die innere Kopfzeilenprüfung wird nicht durchgeführt.

Mit Layer-7-Regeln:

- Snort führt ACP-Prüfungen durch und erzwingt Multi-Layer-Prüfungen.
- Auf die Regelreihenfolge kommt es an (Fehler in Snort 3).
- Wenn die interne IP-Regel vor der L7-Regel → VXLAN-Datenverkehrsunterbrechung erscheint —> Defektes Verhalten

LAB-Ausgabe:
LAB FTD — 7.6.2.1 — snort3 — Innere IP-ACP-Regel gefolgt von L7-Regel — Drop

Details zu Lab Packet Tracer:

17:46:48.773778 10.142.133.15:36066 > 10.126.133.15:4789 udp 80

Inside(vrfid:0)

OBJECT_GROUP_SEARCH

NGIPS-MODUS

| ngips-modus

ZUGRIFFSLISTE

NGIPS-AUSGANGS-SCHNITTSTELLENSUCHE

| Ausgangsschnittstelle auflösen

ERSTELLUNG VON FLÜSSEN

EXTERNE KONTROLLE

SNORT

Typ:

SNORT

Ergebnis:

VERWERFEN

Konfiguration:

Vergangene Zeit:

814472 ns

Zusätzliche Informationen

Ergebnis: verwerfen

Eingangsschnittstelle:

Inside(vrfid:0)

Eingabestatus:

aufstehen

Status der Eingangsleitung:

aufstehen

Ausgangsschnittstelle:

Outside(vrfid:0)

Ausgabestatus:

aufstehen

Status der Ausgabeleitung:

aufstehen

Aktion:

verwerfen

Benötigte Zeit

928908 ns

Ablehnungsgrund:

(Firewall) Durch den Firewall-Präprozessor blockiert <— DROP REASON

Details löschen:

Ablageort: frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow (NA)/NA

Outside(vrfid:0)

- Wenn die L7-Regel vor der internen IP-Regel angezeigt wird → VXLAN-Datenverkehr zulässig

DNS Sinkhole Specific Behavior (Snort 3):

- DNS Sinkhole löst eine mehrschichtige Überprüfung aus, selbst wenn die Regelreihenfolge ansonsten den Datenverkehr zulässt.

Snort 3 (7.6.4+) - Behobenes Verhalten

Nach der Fehlerbehebung (CSCwo54753):

- Multi-Layer-Inspektion wird konsistent aktiviert, wenn L7-Funktionen vorhanden sind.

- Die Regelreihenfolge hat keine Auswirkungen auf das Verhalten.

- Die Datenverkehrsanalyse basiert auf den innersten Headern, unabhängig von der Regelposition.

- Sowohl innere als auch äußere Header müssen in ACP für DNS-Sinkhole-Szenarien zugelassen sein.

Vergleichsmatrix für Testfälle

Testszenario	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Erwartetes Verhalten
L7-Regel gefolgt von Innerer IP-Regel	ZUGELASSEN	ZUGELASSEN	Zulässiger Datenverkehr
Interne IP-Regel gefolgt von L7-Regel	Abgebrochen (Defekt)	ZUGELASSEN	Zulässiger Datenverkehr
Nur interne IP-Regel (kein L7)	Gesperrt	Gesperrt	Gesperrt (Keine innere Berechtigung)
Nur äußere IP-Regel (kein L7)	ZUGELASSEN	Gesperrt	Snort 3 prüft den innersten Header
Nur äußere IP + DNS-	Gesperrt	Gesperrt	Die L7-Regel erzwingt die

Sinkhole			innere Überprüfung.
Nur innere IP + DNS-Sinkhole	Gesperrt	Gesperrt	Die L7-Regel erzwingt die innere Überprüfung.

Ursache

Dieses Verhalten wird durch die Multi-Layer-Inspektionsfunktion von Snort 3 für Security Intelligence-Funktionen verursacht. Wenn DNS Sinkhole (Teil von Security Intelligence) aktiviert ist, führt Snort 3 eine tief greifende Paketprüfung durch, die die innersten IP-Adressen in gekapselten Paketen erkennt und auswertet, unabhängig von der Transportschicht.

Das Problem ist in der Cisco Bug-ID CSCwt12564 dokumentiert, die besagt: "Wenn Sie eine L7-Bedingung (URL-Filterung, App-ID, Geolocation usw.) in der Regel oder eine Sicherheitsdatenfunktion im ACP verwenden, benötigen Sie eine ACP-Regel mit einem inneren Header, damit die Regeln übereinstimmen. Bei dns sinkhole, das Teil der DNS-Richtlinie in SI ist, sind sowohl der innere als auch der äußere Header in einem ACP erforderlich, damit die Regeln übereinstimmen."

Dieses Verhalten unterscheidet sich vom normalen Betrieb, bei dem nur äußere Header für den VXLAN-Transit-Datenverkehr ausgewertet werden, wenn keine Layer-7- oder Sicherheitsinformationsfunktionen konfiguriert sind.

Verwandte Inhalte

- Snort 3 Konfigurationsleitfaden
- Technischer Support und Downloads von Cisco
- Cisco Bug-ID CSCwt12564
- Cisco Bug-ID CSCwt07320
- Cisco Bug-ID CSCwu75396
- Cisco Bug-ID CSCwt58320

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.