根據FMC管理的Firepower裝置的SRU和LSP版本 篩選Snort規則

目錄		
<u>簡介</u>		
<u>必要條件</u>		
<u>需求</u>		
<u>採用元件</u>		
<u>背景資訊</u>		
<u>過濾Snort規則的過程</u>		

簡介

本檔案介紹如何根據Firepower管理中心(FMC)管理的firepower裝置的思科安全規則更新(SRU)和鏈路狀態資料包(LSP)版本過濾snort規則。

必要條件

需求

思科建議您瞭解以下主題:

- 開源Snort知識
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 本文適用於所有Firepower平台
- 執行7.0.0版軟體的Cisco Firepower威脅防禦(FTD)
- Firepower管理中心虛擬(FMC),運行軟體版本7.0.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

在入侵檢測系統(IDS)和入侵防禦系統(IPS)環境中,「SID」表示「特徵碼ID」或「Snort特徵碼 ID」。 Snort特徵碼ID(SID)是分配給規則集內每個規則或特徵碼的唯一識別符號。這些規則用於檢測網路 流量中可能表示惡意活動或安全威脅的特定模式或行為。每個規則都與SID關聯,以便易於參考和 管理。

有關開源Snort的資訊,請訪問<u>SNORT網</u>站。

過濾Snort規則的過程

要檢視Snort 2規則SID,請導航至 FMC Policies > Access Control > Intrusion, 然後點選右上角的SNORT2選項 ,如下圖所示:

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status 🕕	Q Search by Intrusion Policy, De	scription, or Base	All IPS Rules	IPS Mapping Comp	are Policies Create Policy
Intrusion Policy	Description	Base Policy	Usage Information		
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version 📝 🖥 🖆 🗑

Snort 2

導航至 Rules > Rule Update 並選擇最新日期以篩選SID。

Policy Information Rules Cisco Recommendations > Advanced Settings	Rules Rule Configuration Rule Content	Filter:	: Rule Updat	e 2023 04 11 001 vrt"
> Policy Layers	Classifications Microsoft Vulnerabilities Microsoft Worms Diatform Specific	0 selected ru Rule State ▼	les of 2961 Event Fil	tering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
	Preprocessors Priority Rule Update	GID	SID 60221	Message ↑ BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	 Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 04 	1 1	60220 60648	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt BROWSER-CHROME Chrome IPC memory dump attempt
	Changed New	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
	Isp rel 20210503 2107		60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

規則更新

Rules			< Back
Rule Configuration	Filter		
Rule Content	Filter.		
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"		\times
Classifications	0 selected rules of 16		
Microsoft Vulnerabilities			
Microsoft Worms	Policy		
Platform Specific	Rule State Event Filtering Dynamic State Alerting Comments		
Preprocessors			
Priority	GID SID Message ↑	→ ⊕ ▼	' 🕔 🗭 🗭
Rule Update	viviz readme file detected	~	
04 10 001 vrt			î
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow	•
04 1 00 vrt ▼ ∢ ▶		ال < 🗌 1	of 1 \rangle

可用Sid在snort規則下

選擇下面的必需選項 Rule State 如下圖所示。

Rules							<	Back
Rule Configuration Rule Content	Filter:	ule Update 20	23.04.11.001.vrt"				×	20
Classifications Microsoft Vulnerabilities	16 selected rule	6 selected rules of 16						
Microsoft Worms	Policy		•					
Preprocessors Priority	Generate Ever	Event Filterin	g ▼ Dynamic State ▼ Alerting ▼ Comments ▼ ssage ↑	→	● ▼	0	0	-
Rule Update	Drop and Gen	nerate Events	dme file detected	~				
Snort Rule Update 2023 04 11 001 vrt	Disable		-WINDOWS Microsoft Windows AFD.sys privilege escalation	→ < <	1	of	1 >	• >I

選擇規則狀態

要檢視Snort 3規則SID,請導航至 FMC Policies > Access Control > Intrusion ,然後點選右上角的SNORT3選項,如下圖所示:

Intrusion Policies Network	Analysis Policies					
Show Snort 3 Sync status ①	C Search by Intrusion Policy, De	scription, or Base	All IPS Rules	IPS Mapping Compa	are Policies	Create Policy
Intrusion Policy	Description	Base Policy	Usage Information			-
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version	n ∕8¢ i

Snort 3

導航至 Advanced Filters 並選擇最新日期以過濾SID,如下圖所示。

< Intrusion Policy Policy Name FTD1_Intrusion Used by: No Access Control Policy No De								
Mode Prevention Base Policy Balanced Security and Connectivity Disabled 39249 Alert 470 Block 9151 Overridden 0 Rewrite 0 Pass 0 Drop 0 Reject 0								
Rule Groups						Back To Top		
50 items + Q Search Rule Group Excluded Included	All Rules All rules assigned to cu	rrent intrusio	on policy irrespective of rule	group				
Overridden	Rule Action	\sim	Q Search by CVE, SID, R	eference Info, or Rule Message	e			
All Rules Reco	48,870 rules		Preset 470 Alert rules Filters: Advanced Filters	9,151 Block rules 39,249 Di	sabled rules 0 Overridden rules			
> Browser (6 groups)	GID:SID	Info		Rule Action 0	Assigned Groups			
> Server (8 groups)	> 🗌 1:28496 🗹	BROWSER-	IE Microsoft Internet Explore	Alert (Default)	Browser/Internet Explo	B 🗭 🍦		

Snort 3過濾器

r

Advanced Filters

LSP	Select	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	\sim
Microsoft Vulnerabilities	Select	~
	Cancel	OK

a

高級過濾器下的LSP

Advanced Filters				
LSP	Isp rel 20230420 1056 Show Only * 🗹 New 🗹 Changed	~		
Classifications	Select	\sim		
Microsoft Vulnerabilities	Select	~		
	Cancel			
SP版本				
All Rules All rules assigned to current intrusio	n policy irrespective of rule group			
Rule Action 🗸	lsp:lsp rel 20230420 1056 ×	>		
22 🝸 48,870 rules	Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advar	nced Filters		

22 `	22 🝸 48,870 rules Preset Filter		Preset Filters: 0 Alert rules	11 Block rules 11 Disabled rules	0 Overridden rules Advance	d Filters
		GID:SID	Info	Rule Action 0	Assigned Groups	
>		1:300509 📑	MALWARE-BACKDOOR Win.Backdoor	Block (Default)	Malware/Backdoor	B 📕
						_

Sid的預設定篩選器

選擇下面的必需選項 Rule state 如下圖所示。

All Rules All rules assigned to current intrusion policy irrespective of rule group	
Rule Action Isp:lsp rel 20230420 1056 × > 22 22 48,870 rules Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filters	K
GID:SID Info Rule Action O Assigned Groups	
> 🗹 1:300509 🖆 MALWARE-BACKDOOR Win.Backdoor 🕒 Block (Default) 🗸 Malware/Backdoor 🖥 💻	-
	-

規則操作

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。