Filtrare le regole di ordinamento in base all'SRU e alla versione LSP dei dispositivi Firepower gestiti da FMC

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Procedura per filtrare le regole di tipo Snort

Introduzione

In questo documento viene descritto come filtrare le regole di ordinamento in base alla versione Cisco Secure Rule Update (SRU) e Link State Packet (LSP) di dispositivi firepower gestiti da Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort open-source
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo articolo è applicabile a tutte le piattaforme Firepower
- Cisco Firepower Threat Defense (FTD) con software versione 7.0.0
- Firepower Management Center Virtual (FMC) con software versione 7.0.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nel contesto dei sistemi di rilevamento intrusioni (IDS) e dei sistemi di prevenzione delle intrusioni (IPS), "SID" sta per "Signature ID" o "Snort Signature ID".

Il SID (Snort Signature ID) è un identificativo univoco assegnato a ogni regola o firma all'interno del relativo set di regole. Queste regole vengono utilizzate per rilevare modelli o comportamenti specifici nel traffico di rete che possono indicare attività dannose o minacce alla sicurezza. Ogni regola è associata a un SID per semplificare il riferimento e la gestione.

Per informazioni su Snort open-source, visitate il sito Web SNORT.

Procedura per filtrare le regole di tipo Snort

Per visualizzare i SID della regola Snort 2, passare a FMC Policies > Access Control > Intrusion, quindi fate clic sull'opzione SNORT2 nell'angolo superiore destro, come mostrato nell'immagine:

Intrusion Policies Network Analysis Policies								
Show Snort 3 Sync status 🕕	scription, or Base	All IPS Rules IP	PS 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	/80.7		

Snort 2

Passa a Rules > Rule Update e selezionare l'ultima data utile per filtrare il SID.

Policy Information Rules Cisco Recommendations	Rules	Filter:		
> Advanced Settings	 Advanced Settings Policy Layers Policy Layers Rule Content Category Classifications Microsoft Vulnerabilities Microsoft Worms 	SRU:"Snort	t Rule Upda	te 2023 04 11 001 vrt"
> Policy Layers		0 selected ru Rule State ▼	lles of 2961 Event Fi	Itering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
Platform Specific Preprocessors Priority Rule Update Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 04 11 001 vrt Changed	GID	SID	Message 🕆	
	Priority Rule Update	1	60221	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	Snort Rule Update 2021 05 03 001 vrt	1	60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	Short Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 04	1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
	Changed	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Aggiornamento regola

Rules					< Ba	ick
Rule Configuration	Filter					
Rule Content	Filter:					
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"				X	0
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 ↑	->	• •	0		
Rule Update	UIUI2 readme file detected	~				
04 10 001 vrt						-
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow				-
		< <	1	of 1	> >	· I

Sid disponibili sotto snort rules

Selezionare un'opzione richiesta in Rule State come mostrato nell'immagine.

Rules						< Back
Rule Configuration Rule Content	Filter:	000.04.11.001				
Category	SRU:"Snort Rule Update 2	023 04 11 001 vrt"				×
Classifications	16 selected rules of 16					
Microsoft Vulnerabilities	Delieur					
Microsoft Worms	Policy	•				
Platform Specific	Rule State Event Filteri	ng Dynamic State Alerting Comments				
Preprocessors	Conorato Evento					
Priority	Generale Events	sage ↑	\rightarrow	• •	0	••
Rule Update	Drop and Generate Events	time file detected	~			
04 10 001 vrt						î
Snort Rule Update 2023	Disable	-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow			*
<u>04 11 001 vrt</u> →			< > > ا	1	of 1	> >

Selezione degli stati delle regole

Per visualizzare i SID della regola Snort 3, passare a FMC Policies > Access Control > Intrusion , quindi fare clic sull'opzione SNORT3 nell'angolo superiore destro, come mostrato nell'immagine:

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status () C Search by Intrusion Policy, Descr		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 🖍 🖥 🖆 🖡

Snort. 3

Passa a Advanced Filters e selezionare la data più recente per filtrare il SID come mostrato nell'immagine.

< Intrusion Policy Policy Name FTD1_Intrusion			~	Used t	y: No Access Control Policy No Device
Mode Prevention V Base Policy	alanced Security and Con 51 Overridden 0 R	nectivity ewrite 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	irrent intrusi	on policy irrespective of rule group		
Overridden	Rule Action	\sim	Q Search by CVE, SID, Reference Info, or Rule Message		
All Rules Reco	48,870 rules		Preset 470 Alert rules 9,151 Block rules 39,249 Disabled rules 0 Oven Filters: Advanced Filters		es 0 Overridden rules
> Browser (6 groups)	GID:SID	Info	Rule Ac	ction 0	Assigned Groups
> Server (8 groups)	> □ 1:28496 🗹	BROWSER-	-IE Microsoft Internet Explore	ert (Default) 🗸	Browser/Internet Explo 🔹 💻 🖡

Ordina 3 filtri

r

Advanced Filters

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

0

LSP in filtro avanzato

Advanced Fi	ters	0
LSP	lsp rel 20230420 1056	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	\sim
Microsoft Vulnerabilities	Select	~
	Cancel	ĸ
All Rules		
All rules assigned to current intrusic	n policy irrespective of rule group	
Rule Action 🗸	lsp:lsp rel 20230420 1056 ×	2
22 🝸 48,870 rules	Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Av	Ivanced Filters
> 1:300509 🖸 MALWARE-I	BACKDOOR Win.Backdoor Block (Default)	唱 🗭

Filtro preimpostato per SID

Selezionare un'opzione richiesta in $_{Rule\ state}$ come mostrato nell'immagine.

	All Rules All rules assigned to c	current intrusion policy irrespective of rule	e group			
	Rule Action	✓ Isp:Isp rel 20230420 1056	×		X	
Ľ	22 🔽 22 🍸 48,870	0 rules Preset Filters: 0 Alert rules	11 Block rules 11 Disabled rules 0	Overridden rules Advanced Filters		
	GID:SID	Info	Rule Action 0	Assigned Groups		
	> 🗹 1:300509 [MALWARE-BACKDOOR Win.Backdoor	Block (Default)	Malware/Backdoor 🛛 🖥 📕		Î
h						-

Azione regola

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).