

رادصإ ىلإ ادانتسا ل فطتل دعاقوق ةيفصت ممت يتل FirePOWER ةزهجأل LSP و SRU FMC ةطساوب اهترادإ

تايوت حملال

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ريخشل دعاقوق ةيفصت عارجا](#)

ةمدقملا

طابترالال ةلاح ةمزح رادصإ ىلإ ادانتسا ةكبشل دعاقوق ةيفصت ةيفيكن دنتسملال اذه حضوي
ةرادإ زكرم اهريدي يتل FirePOWER ةزهجأل نمو Cisco Secure Rule Update (SRU) نم (LSP)
FirePOWER (FMC).

ةيساسأل تابلطتملا

تابلطتملا

ةيلاتل عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

- ردصملا حوتفم ريخشل ةفرعم
- Firepower (FMC) ةرادإ زكرم
- Firepower Threat Defense (FTD)

ةمدختسملا تانوكملا

ةيلاتل ةيدامل تانوكملا وجماربل تارادصإ ىلإ دنتسملال اذه يف ةدراول تامولعمل دنتست:

- Firepower تاصنم عيجم ىلع ةلاقملا هذه قبطنت
- نم 7.0.0 رادصإ لغشي يذل Cisco نم FirePOWER (FTD) ديدهت دض عافدل جماربل
جمانربلا
- جمانربلا نم 7.0.0 رادصإ لغشي يذل Firepower Management Center Virtual (FMC)

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجأل نم دنتسملال اذه يف ةدراول تامولعمل عاشنإ ممت
تتاك اذإ. (يضاوتفا) حوسمم نيوكتب دنتسملال اذه يف ةمدختسملا ةزهجأل عيجم تادب
رمأ يأل لمتحمل ريثأتلل كمهف نم دكأتف، ليغشتل دي قكتكبش

ةيساسأ تامولعم

"SID" حلطصم ينعي، (IPS) للستل عنم ةمظنأو (IDS) للستل فشك ةمظنأ قايس يف "تروشلا عيقوت فرعم" وأ "عيقوتلا فرعم".

ةومجم نمض عيقوت وأ ةدعاق لكل هنييعة متي ديرف فرعم وه (SID) تروشلا عيقوت فرعم يف ةدجملا تاكولسلا وأ طامألل فاشتكال دعاولل هذه مادختسا متي. هب ةصاخلل دعاولل ةدعاق لك نرتقت. نامأ تاديدهت وأ راض طاشن لىل ريشن أن نكمي يتلا ةكبشلل رورم ةكح ةرادللا وجرلا ةلوهسب حامسلل (SID) نامأل فرعمب.

لىل [SNORT](#) عقوم ةرايزى جري، ردصملا ةحوتفم Snort ةكرش نع تامولعم لىل لوصحللو ببول.

ريخشلا دعاولل ةيفصت ءارجإ

رقنا كلذ دعب، FMC Policies > Access Control > Intrusion، لىل لقتنا 2، Snort ةدعاق ليصوت تاومجم ضرعل ةروصلل يف حضورم وه امك، ينمىللا لىل ةيوازلا يف snort2 رايخ:

Intrusion Policy	Description	Base Policy	Usage Information
FTD1_Intrusion		Balanced Security and Connecti...	No Access Control Policy No Device

2 ترون

(SID) نامأل فرعم ةيفصتل خيرات رخآ ددحو Rules > Rule Update لىل لقتنا

GID	SID	Message
1	60221	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
1	60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

ةدعاقلا شيدحت

Rules < Back

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 0 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: Rule State, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority: GID

Rule Update	SID	Message
04 10 001 vrt	81012	readme file detected
Snort Rule Update 2023 04 11 001 vrt	61615	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

1 of 1

ريخشلل دعاقو تحت ةحاتم ل Sid

ةروصلل ي ف حضورم وه امك Rule State هتحت بولطم رايخ دي دحت

Rules < Back

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 16 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: Rule State, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority

Rule Update

04 10 001 vrt

Snort Rule Update 2023 04 11 001 vrt

04 11 001 vrt

Generate Events

Drop and Generate Events

Disable

Rule Update	SID	Message
04 10 001 vrt	81012	readme file detected
Snort Rule Update 2023 04 11 001 vrt	61615	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

1 of 1

ةدعاقولل تالاج دي دحت

رقنا مٲ ، FMC Policies > Access Control > Intrusion ، ل ل لقتنا ، Snort 3 ةدعاق ل ل صوت تاعومجم ضرعل ةروصلل ي ف حضورم وه امك ، ينم ي ل ل لعلل ةي وازلل ي ف snort3 رايخ

Intrusion Policies Network Analysis Policies

Show Snort 3 Sync status

Search by Intrusion Policy, Description, or Base

All IPS Rules IPS Mapping Compare 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

3 ترون

ةروصلل ي ف حضورم وه امك SID ةي فصتل خيرات رخآ ددحو Advanced Filters ل ل لقتنا

< Intrusion Policy

Policy Name Used by: No Access Control Policy | No Device

Mode 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 Excluded | Included | Overridden

All Rules Reco

> Browser (6 groups)

> Server (8 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

48,870 rules Preset 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules |

Filters: Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
>	<input type="checkbox"/> 1:28496	BROWSER-IE Microsoft Internet Explore...	<input type="text" value="Alert (Default)"/>	Browser/Internet Explo...

Snort 3 ةيفصت لماع

Advanced Filters ?

LSP

Select...

Show Only * New Changed

Classifications

Select...

Microsoft
Vulnerabilities

Select...

Cancel

OK

مدقت م ةيفصت لماع تحت LSP

Advanced Filters



LSP

Isp rel 20230420 1056

Show Only * New Changed

Classifications

Select...

Microsoft

Vulnerabilities

Select...

Cancel

OK

LSP رادصا

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 | 48,870 rules | Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

Sid's لة قبسم ةومجم ةيفصت لماع

ةروصل ايف حضورم وه امك Rule state هتحت بولطم راوخ ديدحت

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 | 22 | 48,870 rules | Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input checked="" type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input checked="" type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل