

ةيكلولسلل تاريغتلل نم ققحتلل ةيفيك عيقوت ةمزح ثيدحت دعب IPS تاعيقوت يف ةديج

تايوتحملل

[ةمدقملل](#)

[ةيساسألل تابللطتلل](#)

[تابللطتلل](#)

[ةمدختسملل تانوكملل](#)

[ةلكشملل](#)

[لحلل](#)

[ةلصلل تاذ Cisco معد عم تجم تاشقانم](#)

ةمدقملل

ثيدحت دعب ةديجلل تاعيقوتلل اهتلخدأ يئلل ةيكلولسلل تاريغتلل دنن سملل اذه فصوي
ةديج عيقوت ةمزح لىل Cisco نم (IPS) لىلستلل عنم ماظن.

ةيساسألل تابللطتلل

تابللطتلل

ةيلالل عيضاوملل اب ةفرعم كيدل نوكت نأب Cisco ي صوت:

- IPS لىل عيقوتلل ثيدحت ةزيم

ةمدختسملل تانوكملل

ةيلالل ةيداملل تانوكملل او جماربلل تارادصلل لىل دنن سملل اذه يف ةدراولل تامولعملل دننست:

- IPS 4xxx Series راعشتسالا ةزهجأ
- ASA 5585-X IPS SSP ةلسلس
- ASA 5500-X IPS SSP ةلسلس
- ASA 5500 IPS SSM ةلسلس

رادصلل 7.1(10)E4

رادصلل 7.3(4)E4

[تالطصلا لوح تامولعملل نم ديزم لىل لوصحلل ةينقتلل Cisco تالطصلا عجار
تادنن سملل](#)

ةلكشملل

تاقېب طت عم لاصتالال كاشموم مزحلال طاقسإ تالاح لثم ةددعتم لكاشم كانه نوكت دق نوكتيس، اهالصالال كاشملا هذه اطاخأ فاشكتسال. IPS لعل عي قوت شي دحت ارجا دعب ةني عم شي دحت دعب ةطشنلال عي قوتلال ةومجم يف تاريخي غتلال مهف لعل ارداق تنك اذا ارج دي فملا نم عي قوتلال.

لحل

1. ةوطخلال

عي قوتلال ةمزح ربخي اذه. عي قوتلال ةي قرتلال تاظوفحم وه هنم ققحتلال لىل اجاتحت عيش لوأ عي قوتلال ةمزح نم يلالحال رادصالال او IPS لعل لمعت تنك يلال ةقباسلال

show يف ةي قرتلال تاظوفحم مسق نم وأ show version رمألا ارجا نم كلذ لىل روثلال نكم يو لاقملا سفن نم فطتقم عجل لىل انه راشي. tech.

ةي قرتلال تاظوفحم

* IPS-SIG-S733-Req-E4 19:59:50 UTC FRI 09 2015 س طس غأ

IPS-SIG-S734-req-E4.pkg 19:59:49 UTC TUE 13 2015 س طس غأ

تمت و s733 تنك IPS لعل لمعت تنك يلال ةقباسلال عي قوتلال ةمزح نأ حضوت نأ كنكمي نألا ةي لالحال عي قوتلال ةمزح يه يلال او s734 لىل اهتي قرت

2. ةوطخلال

نم اهنم ققحتلال نكمي يلال او اءارچ مت يلال تاريخي غتلال مهف يف ةي نالال ةوطخلال لثمتتو لال IME/IDM.

ةروصلال هذه يف IME/IDM يف "طشنلال عي قوتلال" بيوبتلال ةمالع ضرع متي 1.

ةطشنلال تاعي قوتلال > SIG1 > عي قوتلال تافيرعت > تاسايسلال > نيوكتلال لىل لقتنا

Cisco IDM 7.3 - 10.105.130.100

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Policies Configuration > Policies > Signature Definitions > sig1 > Active Signatures

Threat Profile Edit Actions Enable Disable Restore Default MySDN Edit Add Delete Clone Export

Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Alert and Log	Deny	Other	Type	Engine	Retired
1000/0	IP options-Bad Option List	<input checked="" type="checkbox"/>	High	75	18	Alert			Default	Atomic IP	Active
1006/0	IP options-Strict Source Route	<input checked="" type="checkbox"/>	High	100	100	Alert			Default	Atomic IP	Active
1018/0	Lurk Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert			Default	String TCP	Active
1019/0	XShellC601 Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert			Default	String TCP	Active
1020/0	BB Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert			Default	String TCP	Active
1021/0	Murcy Malware Communication	<input checked="" type="checkbox"/>	Medium	85	63	Alert			Default	Service HTTP	Active
1022/0	QDigit Malware Communication	<input checked="" type="checkbox"/>	Medium	95	71	Alert			Default	String TCP	Active
1027/0	Cisco IOS Software Smart Install Denial of Service	<input checked="" type="checkbox"/>	Medium	80	60	Alert			Default	String TCP	Active
1030/0	Symantic TM Manager Administrator Console Code ...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	Service HTTP	Active
1032/0	Microsoft Windows MPEG Layer-3 Audio Decoder S...	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1039/0	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	Multi String	Active
1039/1	Microsoft Windows Remote Desktop Protocol Vulne...	<input checked="" type="checkbox"/>	High	80	80	Alert			Default	Multi String	Active
1040/0	DNSChanger Malware	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	Atomic IP	Active
1044/0	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/1	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP XL	Active
1044/2	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/3	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/4	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/5	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/6	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/7	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/8	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/9	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1044/10	Metasploit Shellcode Encoder	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP XL	Active
1051/0	Novell GroupWise Internet Agent HTTP Request R...	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	String TCP	Active
1052/0	Adobe PDF Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1055/0	Cisco WebEx WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	Multi String	Active
1057/0	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1057/1	Cisco WebEx Player WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1058/0	Cisco Webex WRF File Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	Multi String	Active
1080/0	IBM Informix Long Username Buffer Overflow	<input checked="" type="checkbox"/>	High	95	95	Alert			Default	String TCP	Active
1088/0	Oracle XDB FTP Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active
1101/0	Unknown IP Protocol	<input checked="" type="checkbox"/>	High	75	18	Alert			Default	Atomic IP	Active
1102/0	Impossible IP Packet	<input checked="" type="checkbox"/>	High	100	100	Alert			Default	Atomic IP	Active
1104/0	IP Localhost Source Spoof	<input checked="" type="checkbox"/>	High	100	100	Alert			Default	Atomic IP	Active
1127/0	Cisco IOS ISAKMP Vulnerability	<input checked="" type="checkbox"/>	High	85	85	Alert			Default	Atomic IP	Active
1134/0	Microsoft IE SelectAll Remote Code Execution	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	Multi String	Active
1140/0	Samba Marshalling Code Remote Code Execution V...	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	Service SMB A...	Active
1184/0	Adobe Acrobat Reader Buffer Overflow	<input checked="" type="checkbox"/>	High	90	90	Alert			Default	String TCP	Active

2. ددحم عي قوت رادصل ديدحت ةيفيك ةروصل هذه حضوت .

تارادصل ال > SIG1 > عي قوت ال تافيرت > تاسايس ال > نيوكت ال ال لقتنا .

Cisco IDM 7.3 - 10.105.130.100

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Policies Configuration > Policies > Signature Definitions > sig1 > Releases

Select: 5741 Filter: Sig Name

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions			Type	Engine	Retired
						Alert and Log	Deny	Other			
2725/0	Denial Of Service	<input checked="" type="checkbox"/>	Medium	90	67	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Active
2732/0	Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2736/0	Theme Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
2744/0	Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2747/0	Internet Explorer Memory Corr...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2765/0	Microsoft FrontPage Information Disclosure	<input checked="" type="checkbox"/>	Medium	80	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Active
2769/0	Microsoft Active Directory LDAP Service Denial of S...	<input checked="" type="checkbox"/>	Medium	85	63	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Atomic IP	Active
2771/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	80	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2772/0	Microsoft Sharepoint XSS Elevation of Privilege	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	Service HTTP	Low Memory Retired
2773/0	Microsoft Internet Explorer Use After Free	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2774/0	Microsoft Internet Explorer Memory Corruption Vul...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2775/0	Microsoft Windows Internet Explorer Memory Cor...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
2777/0	Microsoft Internet Explorer Use After Free Vulnera...	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
4155/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired
4156/0	Microsoft Internet Explorer Remote Code Execution	<input checked="" type="checkbox"/>	High	85	85	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	String TCP	Low Memory Retired

ىلع ءانب اهتيفصت كنكمي، نيعم رادصا نم هيلع تلصح يذلا حشرملا راىخ مادختساب هخا ىل، ةروطخلا، ةقدلا، كرحملا

عيقوتلا رادصا يف تاريغتلا قييضت ىلع ارداق نوكت نا بجي، كلذب مايقلا لالخنم فاشكتسا اذاحمب اهساسا ىلع موقت يتلا ةلكشملا الم تحم اببس نوكت نا نكمي يتلا اهالصل او عاطخالا

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل