

Cisco é © Ā;œāž<ā,»ā,āf¥āf^aāftā,£

ā,čāf—āf©ā,āā,čāf³ā,¹

ā,½āf•āf[^]ā,|ā,šā,čā Šā,^ā³ Firepower

Threat Defense

ā,½āf•āf[^]ā,|ā,šā,čā © ä½Žā,“āf³āf[^]āfāf’āf¼

ā,āf¼ā © è,,tā¼±æ€š



ā,čāf%āfā,ā,ā,āfāf¼ID : cisco-sa-

[CVE-2023-](#)

asa5500x-entropy-6v9bHVYP

[20107](#)

ā[^]ā...-é-^æ-¥ : 2023-03-22 16:00

āfāf¼ā,āfšāf³ 1.0 : Final

CVSSā,¹ā,³ā,č : [5.3](#)

ā>žéžç- : Yes

Cisco āfā,° ID : [CSCvm90511](#)

æ—¥ææ-è^ažā «ā,^ā,<æf...ā ±ā -ā€ è<±è^ažā «ā,^ā,<āŽŸæ-†ā © éžā...-ā¼ā

æ!,è!?

Cisco ASA 5506-Xā€ASA 5508-Xā€ā Šā,^ā³ASA 5516-

Xāf•ā,;ā,ā,čā,|ā,©āf¼āf«ç””ā ©Cisco Adaptive Security

Appliance(ASA)ā,½āf•āf[^]ā,|ā,šā,čā Šā,^ā³Cisco Firepower Threat

Defense(FTD)ā,½āf•āf[^]ā,|ā,šā,čā ©Deterministic Random Bit

Generator(DRBG)ā ©è,,tā¼±æ€šā «ā,^ā,Šā€è^aè”¼ā•ā,Čā |ā,,ā^aā,,āfāfčāf¼āf[^]ā ©

ā “ā ©è,,tā¼±æ€šā -ā€æš-ā•ā,āf¼ā,’ç”Ÿæ[^]āTMā,<és>ā «ā€è²ā½”āTMā,<āfāf¼āf%ā

āf†āfā,ā,ā,¹ā “ā ©ā,€è†ā,’æŽčāTMā “ā “ā «ā,^ā,Šā€ā “ā ©è,,tā¼±æ€šā,’ā,“ā,ā,āf

āf†āfā,ā,ā,¹ā «ā^aā,ŠāTMā³ā -ā Ÿā,Šā€è²ā½”ā ©ā,žāf¼ā,²āffāf[^]

āf†āfā,ā,ā,¹ā “ā ©é-“ā Šé€äž;ā•ā,Čā,<è²ā½”ā ©ā,āf¼ā Šāž è-ā•ā,Čā |ā,,ā,<āf[^]ā

ā,ā,¹ā,³ā -ā “ā ©è,,tā¼±æ€šā «ā³ā†|āTMā,<ā,½āf•āf[^]ā,|ā,šā,čā,čāffāf—āf†āf¼āf[^]ā,’ā^aāf^aāf¼

ā “ā ©ā,čāf%āfā,ā,ā,āfā^a -ā€æ-;ā ©āfāf³ā, -ā,^ā,Šçç^oè^aā ŠāTMā³āTMā€,

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa5500x-entropy-6v9bHVYP>

Cisco ASA	
VPNi^WebVPNi%	enable <interface_name>
IKEv1 VPNi^af^af^af^af^ ã, çã, -ã, »ã, 1ã Šã, ^ã^3 LAN-to-LANI% è`¼æ~Žæ>, ãf™ãf¼ã, 1ã®è^è`¼ã, 'ã½ç'''	crypto ikev1 enable <interface_name> crypto ikev1 policy <priority> authentication rsa-sig tunnel-group <tunnel_group_name> ipsec-attributes trust-point <trustpoint_name>
IKEv2 VPNi^af^af^af^af^ ã, çã, -ã, »ã, 1ã Šã, ^ã^3 LAN-to-LANI% è`¼æ~Žæ>, ãf™ãf¼ã, 1ã®è^è`¼ã, 'ã½ç'''	crypto ikev2 enable <interface_name> tunnel-group <tunnel_group_name> ipsec-attributes ikev2 remote-authentication certificate ikev2 local-authentication certificate <trustpoint_name>
ãfãf¼ã, «ãf«è^è`¼ã±€i¼^CAi¼%	crypto ca server no shutdown
Mobile Device Manageri¼^MDMi¼%ãf—ãfã,ã,·	mdm-proxy enable <interface_name>
ãfçãf^ã, ããf«ãf!ãf¼ã, ¶ ã, »ã, ãfãfãfãfã, €i¼^MUSi¼%	webvpn mus password <password> mus server enable port <port #> mus <address> <mask> <interface_name>
Proxy Bypass	webvpn proxy-bypass
REST API ¹	rest-api image disk0:<image name> rest-api agent
SSHã, çã, -ã, »ã, 1ã^3	ssh <remote_ip_address> <remote_subnet_mask> <interface_name>

1. ASDMã€CSMã€ãŠã, ^ã^3 REST API ã, ãf¼ãf"ã, 1ã-ã€ http

ã, ãfžãfãf%ãŠè`¼ãŠãã,ã, ÇããŸç`„ã>²ã® IP

ã, çãf%ãf-ã, 1ã<ã, %ã®ãçã, çã, -ã, »ã, 1ãŠãããã¼ã™ã€,

2. SSH ã, ãf¼ãf"ã, 1ã-ã€ ssh ã, ãfžãfãf%ãŠè`¼ãŠããã,ã, ÇããŸç`„ã>²ã® IP

ã, çãf%ãf-ã, 1ã<ã, %ã®ãçã, çã, -ã, »ã, 1ãŠãããã¼ã™ã€,

3.

SSHã, çã, -ã, »ã, 1ã«ã³ãã™ã,ãã"ã®è,, tã¼±æ€šã«ã³ã†!ã™ã,ã>žéçç-ã-ã,ã,Šãã¼ã

FTD ã, ãfãfãfã, ã, šã, ç

æ-¼ã®è;ãŠãã-ã€ã!ã®ã-ã«ã€è,, tã¼±æ€šãÇããæ`ã™ã,ãã-èf½æ€šãÇãã

FTDã€Ÿèf½ã, ççªã-ãã¼ã™ã€,ãã¼ãŸãã®ã-ã«ã-ã€show running-

config CLI

1. `anyconnect ssl vpn enable` `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

Cisco FTD	<code>anyconnect ssl vpn enable</code>
AnyConnect SSL VPN	<code>anyconnect http server enable</code>
AnyConnect SSL VPN WebVPN	<code>anyconnect ikev1 enable</code>
HTTP	<code>anyconnect ikev2 enable</code>
IKEv1 VPN LAN-to-LAN	<code>anyconnect ssh</code>
IKEv2 VPN LAN-to-LAN	
SSH	

1. `anyconnect ssl vpn enable` `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

2. `anyconnect ssl vpn enable` `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

3. `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

4. `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

5. `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

6. `anyconnect http server enable` `anyconnect ikev1 enable` `anyconnect ikev2 enable` `anyconnect ssh`

è,,†â¼±æ€\$ã, 'â€«ã,"ã€šã,,ã€ªã,,ã€"ã€ "ã€œçç°èªã€•ã,œã€ÿè£½ã"€

ã€"ã€®ã,çãf%ããã,ã,¶ã,¶ãã€®è,,†â¼±æ€\$ã€®ã€,ã,«è£½ã"€ã,»ã,¬ã,ããšãã€«è~è¼%ã€•ã

ã,ã,¹ã,³ã€¬ã€ã€ã€ã€®è,,†â¼±æ€\$ã€œæ¬ã€®ã€—ã€œã€œã€ªã€ã,œã€¼ã€ã€šã€ÿè;œã€•ã,œ
Cisco ASAã,½ããªãªã,|ã,šã,çã€¾ã€ÿã€¬FTD

ã,½ãªãªãª,|ã,šã,çã€«ã½±éÿã,ã,žã€ªã€ª,,ã€"ã€ "ã€,çç°èªã€—ã€¾ã€—ã€ÿã€,

- 3000ã,ãªãª¼ã,°ç"£æÿç""ã,»ã,ãªãªªãªªãª,£ã,çãª—ãªœã,ãã,çãª³ã,¼¹^ISAi¼%
- ASA 5525-Xã€œ5545-Xã€œ5555-Xã€œã€šã,^ã€³5585-Xã,»ã,ãªãªãªãªãª,£ã,çãª—ãªœã,ãã,çãª³ã,¹
- Cisco Catalyst 6500ã,ãªãª¼ã,°ã,¹ã,ãªãªãªã€ã€šã,^ã€³Cisco 7600ã,ãªãª¼ã,°ãªãª¼ã,çç""ã€® ASAã,µãª¼ãªã,¹ãªçã,ãªãªãªãªãªãª
- é€œœãªœãžã,ã,ãªãªãªãªãª,£ãªªãª¼ãªªãª£ãªª«ã,çãª—ãªœã,ãã,çãª³ã,¼¹^ASAã¼%œ
- Firepower 2100ã,ãªãª¼ã,°
- Firepower 4100ã,ãªãª¼ã,°
- Firepower 9300ã,ãªãª¼ã,°
- Firepower Threat Defense Virtual(FTDv/NGFWv)
- Cisco Secure Firewall 3100ã,ãªãª¼ã,°

ãªžé€ç-

SSL/TLSªœÿè£½ã€®ã€çã€šã½çç""ã€•ã,œã,«æš—ã€ã,ãª¼ã€«ã¾ã€—ã€|ã€ã€ã€"ã€®è,,†â¼

è,,†â¼±ã€ªæš—ã€ã,ãª¼ã€®ã½çç""ã,ãªžé€çã€ªã,ã€«ã€¬ã€Cisco

ASAã¾ã€ÿã€¬Cisco

FTDãªãªãª,ãª,¹ã»ãªã—ã€®ãªçé¼ã€šã€ã,«ãªãªãªãª,ãª,¹ãšã,ãª¼ãªãšã,çã€¬ã¾ãªœã€ªã,«è¼

ca import <trust-point-name> pkcs12

<passphrase>ã,ãªãªãªªãªª,¹ã½çç""ã—ã€|ã€ã€ã,ãª¼ã€"è¼æ~žæ,ã,ã€«ã,œBase

64ã,¹ãª³ã,ãªãªãªª%PKCS #12ãª,ãª,ãªãª«ã,Cisco ASAã¾ã€ÿã€¬Cisco

FTDãªãªãªãª,ãª,¹ã«ã,ãªãªãªãªãªãª—ã¾ã€ªãªª,ª

Cisco Adaptive Security Device

Manager(ASDM)ã,¹ã½çç""ã—ã€|ã€"ã€®ã,ãª,¹ã,¬ã,¹ã®ÿè;œã€ªã,«æ%œéãª,ã€«ã,œè³ç°ã€«ã€

8.x:ASDMã,¹ã½çç""ã—ã€ÿSSLe"¼æ~žæ,ã€®æ'æ°ã€"ã,ãªãªã,¹ãªãª¼ãªªãªã€ã,¹ã,ç...šã—ã€

ã€"ã€®ãªžé€ç-ã€¬ãªžã...ãªã,œã€|ã€šã,šã€ãªªã,¹ãªãª°ãªãªšã€¬ã®ÿè¼æ,¹ãªçãªã

ãªœ£æ,^ã€çã,½ãªãªãª,|ã,šã,ç

ã,½ãªãªãªãª,ã,šã,çã€®ã,çããªãª—ã,°ãªãªãª¼ãªª%ã,¹ãªªœè~žã€ªã,«éšã€«ã€¬ã€ã,ã,¹ã,³

⌘æ£â^©ç™"ä°<ä¾<ã⌘ "å...¬å¼⌘ç™°èj™

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ã⌘ ¯ã€⌘æœ¬ã,çãf%ãf⌘ã,ãã,¶ã,¶ãfãã⌘«è™~è¼%ã⌘•ã,CEã⌘ |ã⌘,,ã,«è,,†å¼±æ€šã⌘

å†°å... ,

ã,·ã,¹ã,³ã⌘ ¯ã€⌘ã⌘"ã⌘@è,,†å¼±æ€šã, 'å ±å'šã⌘—ã⌘ |ã⌘,,ã⌘ÿã⌘ã⌘,,ã⌘ÿANSI/CERT-
FRi¼^ãf·ãf©ãf³ã,¹ã⌘@å>½ã⌘šã, ^ã⌘³æ"¿å°œã⌘@CSIRTi¼%ã⌘«æ,,ÿè¬ã⌘,,ã⌘ÿã⌘—ã⌘¾ã⌘™æ€

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa5500x-entropy-6v9bHVYP>

æ™¹è™,å±¥æ´

ãf⌘ãf¼ã,ãfšãf³	èª¬æ~ž	ã,»ã,¬ã,·ãfšãf³	ã,¹ãf†ãf¼ã,¿ã,¹	æ—¥ã»~
1.0	å^⌘å>žå...¬é¬ãfããf¼ã,¹	-	Final	2023å¹³æœ²2æ—¥

å^©ç™"è!⌘ç´,,

æœ¬ã,çãf%ãf⌘ã,ãã,¶ã,¶ãfãã⌘ ¯ç,,jã¿⌘è™¼ã⌘@ã,,ã⌘@ã⌘ "ã⌘—ã⌘ |ã⌘"æ⌘⌘ã¾ã⌘—ã⌘ |ã⌘šã,šã€
æœ¬ã,çãf%ããf⌘ã,ãã,¶ã,¶ãfãã⌘@æf...å ±ã⌘šã, ^ã⌘³ãfããf³ã,¬ã⌘@å½çç™"ã⌘«é¬çã⌘™ã,«è²¬ã»ã⌘@ã,€
ã⌘¾ã⌘ÿã€⌘ã,·ã,¹ã,³ã⌘ ¯æœ¬ãf%ãã,ãfããf;ãf³ãf^ã⌘@å†...å@¹ã,'å°^å'šã⌘ªã⌘—ã⌘«å°œ%æ>ã⌘—ã⌘
æœ¬ã,çãf%ããf⌘ã,ãã,¶ã,¶ãfãã⌘@è™~è¿°å†...å@¹ã⌘«é¬çã⌘—ã⌘ |æf...å ±é...⌘ã¿jã⌘@ URL
ã,'çœçç·¥ã⌘—ã€⌘å⌘~ç<¬ã⌘@è»çè¼%ãã,,æ,,⌘è™³ã,'æ¬½ã⌘—ã⌘ÿã 'å⌘^ã€⌘å½"ç¾¾ã⌘CEç@jç⌘
ã⌘"ã⌘@ãf%ãã,ãfããf;ãf³ãf^ã⌘@æf...å ±ã⌘ ¯ã€⌘ã,·ã,¹ã,³è£½å"⌘ã⌘@ã, "ãf³ãf%ããf,ãf¼ã,¶ã, 'å³¼è±jã

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。