

èœ†æ•°ã ®ã,·ã,¹ã,³è£½å" ®ã,µãf¼ãf ®ã ®

Identification Data

Exfiltrationã ®è,,†å¼±æ€§



ã,çãf%ãf ®ã,µã,¶ãfãf¼ID : cisco-sa-sni- [CVE-2021-34749](#)

data-exfil-mFgzXqLN

å^ ®å...-é-æ—¥ : 2021-08-18 16:00

æ€œæ'æ-°æ—¥ : 2021-09-27 16:31

ãf ®ãf¼ã,ãfšãf³ 1.1 : Interim

CVSSã,¹ã,³ã,ç : [5.8](#)

åžé ®ç- : No workarounds available

Cisco ãf ®ã,° ID : [CSCvy50873](#) [CSCvz34379](#)

[CSCvy64824](#) [CSCvy76771](#)

æ—¥æ-èªžã ®«ã,^ã,æf...å ±ã ®-ã€ ®è±èªžã ®«ã,^ã,æžÿæ-†ã ®é ®žã...-å¼ ®ã ®

æ!,è! ®

èœ†æ•°ã ®ã,·ã,¹ã,³è£½å" ®ã ®Webãf·ã,£ãf«ã,çãfãf³ã,°æ©ÿèf½ã ®è,,†å¼±æ€§ã ®«ã,^ã,šã€ ®èª ®

ã ®"ã ®è,,†å¼±æ€§ã ®-ã€ ®SSL/TLSãf ®ãfãf%ã,·ã,šã,µã, -ã ®«ã ®šã ®ã,æ,µãf¼ãf ®å ®è~å^¥(SN

æ-;ã ®Snortãf«ãf¼ãf«ã,'å½ç" ®ã ®—ã ®!ã€ ®ã ®"ã ®è,,†å¼±æ€§ã ®ã,æfå^©ç" ®ã ®å ®-èf½
SID 58062ã€,

ã ®"ã ®è,,†å¼±æ€§ã ®«ã ®¾å†!ã ®™ã,æžé ®ç-ã ®-ã ®,ã,šã ®¾ã ®ã,"ã€,

ã ®"ã ®ã,çãf%ãf ®ã,µã,¶ãfãf¼-ã€ ®æ-;ã ®ãfãfãfã, -ã,^ã,šçç°èª ®ã ®šã ®ã ®¾ã ®™ã€,

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sni-data-exfil-mFgzXqLN>

è©²å¼"è£½å" ®

è,,†å¼±æ€§ã ®ã ®,ã,è£½å" ®

å...-é-æ™,ç,¹ã ®šã ®-ã€ ®ã ®"ã ®è,,†å¼±æ€§ã ®-ãfãfãf¼ã,¹2.9.18ã,^ã,šã%ã ®ã ®ã ®™ã ®¹ã

å...-é-æ™,ç,¹ã ®šã ®-ã€ ®æ-;ã ®ã,·ã,¹ã,³è£½å" ®ã ®SSL/TLSå¾©å ®å ®æ-ã,ªãf-ã,ãfšãf³ã,'å½

- 3000 ā, ·āf^aāf^{1/4}ā, °ç”£æŸç””ā, »ā, āfŸāf^aāf†ā, £ ā, çāf—āf©ā, ¢ā, çāf³ā, i^{1/4}^ISAi^{1/4}%o
- 4000ā, ·āf^aāf^{1/4}ā, °ā, āf^{1/4}āf[“]ā, °ç#ā^âžāf«āf^{1/4}ā, ž(ISR)i^{1/4}^4321 ISRā, 'é™āā^âi^{1/4}%o
- Catalyst 8000V ā, °āfā, , ā, 1/2āf·āf^ā, lā, šā, ç
- Catalyst 8200 ā, ·āf^aāf^{1/4}ā, ° ā, °āfā, , āf—āf©āfāf^āf·ā, ©āf^{1/4}āf
- Catalyst 8300 ā, ·āf^aāf^{1/4}ā, ° ā, °āfā, , āf—āf©āfāf^āf·ā, ©āf^{1/4}āf
- Cloud Services Router 1000Vā, ·āf^aāf^{1/4}ā, °(CSR 1000V)
- Firepower Threat Defense(FTD)ā, 1/2āf·āf^ā, lā, šā, çⁱ1/4^SSL/TLSā^{3/4}©ā^â·āCE—ā, °āf—ā, ·āfšāf³ā^âCEæœ%oāš¹ā^âā[’]ā^â
- ā, āf^{1/4}āf[“]ā, °ç#ā^âžāf«āf^{1/4}ā, ži^{1/4}^ISRvi^{1/4}%o
- Webā, »ā, āfŸāf^aāf†ā, £ā, çāf—āf©ā, ¢ā, çāf³ā, °(WSA)i^{1/4}^ç%o©ç^âtāf†āf^âā, ¢ā, 1ā^â”ā»@æf³āf†āf^â

ā...¬é—æ™, ç, 1ā^âšè, †ā^{1/4}±æ€šā^âCEç[°]è^aā^â·ā, CEā^â|ā^â, ā, < Cisco
 ā, 1/2āf·āf^ā, |ā, šā, çā^â@āf^aāf^{1/4}ā, 1ā^â«ā^âā^â, ā^â|ā^â—ā€ā^â”ā^â@ā, çāf%oāf^âā, ¢ā, ¶āfā^â@
 ID ā^â@è³ç[°]ā, »ā, ā, ·āfšāf³ā, ā^â, ç...šā^â—ā^â|ā^âā^âā^â·ā^â, ā^â,

FTDā^â«é—çā^â™ā, ā^âā^â@ā^â—ā^â@è€fæ...@ā[°]é ...

FTDāf†āf^âā, ¢ā, 1ā, 'è, †ā^{1/4}±ā^â«ā^â™ā, ā^â«ā^â—ā€ā[°]ā^âā^âā^â”ā, 1ā^âā^â@SSLā^{3/4}©ā^âā^âCE—

Cisco

FTDā, 1/2āf·āf^ā, lā, šā, çā^â@SSLā^{3/4}©ā^â·āCE—āf^âāf^aā, ·āf^{1/4}ā^âCEæœ%oāš¹ā^â«ā^âā^â£ā^â|ā^â, ā,

SSL

ā^{3/4}©ā^â·āf^âāf^aā, ·āf^{1/4}ā^âCEæœ%oāš¹ā^â«ā^âā^â£ā^â|ā^â, ā, ā^âā^â©ā^âtā^âā^â—ā€ā^âæ¬ā^â@
 2 ā^âā^â@æ⁻¹æ³·ā^âšç[°]è^aā^âšā^âā^âā^{3/4}ā^â™ā€,

ā, °āf—ā, ·āfšāf³ i^{1/4}šCLI ā^â@ā^{1/2}ç””

CLI ā, °āfžāf³āf%oā^â@ show ssl-policy-config ā, 'ā^{1/2}ç””ā^â—ā^â|ā€ā^âf†āf^âā, ¢ā, 1ā^âš SSL
 ā^{3/4}©ā^â·āf^âāf^aā, ·āf^{1/4}ā^âCEæœ%oāš¹ā^â«ā^âā^â£ā^â|ā^â, ā, ā^âā^â©ā^âtā^âā^â, 'ç[°]è^aā^â—
 āf^âāf^aā, ·āf^{1/4}ā^âCE”ā^â@šā^â·ā, CEā^â|ā^âšā, %oā^âšā€è, †ā^{1/4}±æ€šā^âCEā[~]æœ”ā^â—ā^âā^â, āf†āf^â
 show ssl-policy-config ā, °āfžāf³āf%oā^â@ā[°]āš[°]ā, 'ç[°]ā^â—ā^âā^{3/4}ā^â™ā€,

<#root>

>

show ssl-policy-config

SSL policy not yet applied.

show ssl-policy-config

SSL

show ssl-policy-config

GUI

SSL

Firepower

- [Firepower Management](#)

Centeri^FMCi^%o

[Policies] > [Access Control]

- [Firepower Device](#)

Manageri^FDMi^%o

[Policies] > [SSL Decryption]

WSA

WSA

WSA

Web

HTTPS

HTTPS

WSA

WSA

WSA

WSA

- 1000
- 4321
- é
- Catalyst 8500
- Firepower Management Centeri^FMCi^%o

- Merakiä, »ã, äfÿäfäf†ã, £ã, çãf—ãf©ã, mã, çãf³ã, 1ã€ã... ”ãfçãf†ãf«
- ä, äf¼ãf—ãf³ã, ½ãf¼ã, 1Snort 3
- Umbrella

è©³ç°

ãf³ãfçãf¼ãf^æ”»æ’fè€...ã—ã€SNICatãã¼ãYã—ãCEæS~ã®ãf,,ãf¼ãf«ã,’ã½ç””ã—ã|ã€ã
ã”ã®ã, çãf%ããfã, mã, ¶ãfãSã—ã€Webãf-ãf”ãfÿãf†ãf¼ã, ·ãfSãf³ãfã, £ãf«ã, çã€URLãfã, £ã
ã®ã®ã®é-”ã€SNICatãf,,ãf¼ãf«ãSã®Yè;CEã•ã, CEã, «æ”»æ’fã, ’æœœã†°ã—ã|è»½æ, >ã™ã, <ã
ã«è”ã®šã™ã, <ã½...è|ãCEã, ã, Šã¼ã™ã€,

ã»žéç-

ç%ã¹ã®šã®Ciscoè£½ã”ã«ã¼ã™ã, <ãžéç-ã«ããã,,ã|ã—ã€ã”ã®ã, çãf%ããfã,

äç®æ£æ, ^ãçã, ½ãfãf^ã, |ã, Šã, ç

[ã, ½ãfãf^ã, |ã, Šã, çã®ã, çãffãf—ã, °ãf-ãf¼ãf%ã, ’æœœè”Žã™ã, <észã«ã—ã€ã, .ã, 1ã, 3](#)
[ã, »ã, äfÿãfãf†ã, £ã, çãf%ããfã, mã, ¶ãfã](#)
[ãfSãf¼ã, ãSã...ÿæ%ããSããã, <ã, ·ã, 1ã, 3è£½ã”ã®ã, çãf%ããfã, mã, ¶ãfã, ’ã®šæœYçš,,ã«ã, ç](#)
ã, ½ãfãfÿãf¼ã, ·ãfSãf³ã, €ã¼ã, çç°èãã—ã|ã®ããããã•ã,,ã€,

ã,,ãšã, CEã®ã’ã^ã,,ã€ã, çãffãf—ã, °ãf-ãf¼ãf%ãã™ã, <ãf†ãfã, mã, 1ã«ããã^tãããfãfãçã
Technical Assistance
Centeri¼TACi¼%ã,,ã—ã®ãã—ãÿç’,ã—ã|ã,,ã, <ãfãf³ãf†ãfŠãf³ã, 1ãf—ããfã, mãfãf¼ã«

äç®æ£æ, ^ãçãfãfãf¼ã, 1

[äç®æ£æ, ^ãçã, ½ãfãf^ã, |ã, Šã, çãfãfãf¼ã, 1ã®è©³ç°ã«ããã,,ã|ã—ã€ã”ã®ã, çãf%ããfã](#)

ä, æ£ã^©ç””ã°<ã¼ãã”ã...-ã¼ç™°è;”

Cisco Product Security Incident Response
Teami¼^PSIRTi¼%ã—ã€ã, çãf%ããfã, mã, ¶ãfãSèª-æ~Žã•ã, CEã|ã,,ã, <è,,tã¼±æ€Sã«ã¼ãã
ã, ½ãfãf%ããCEã...ÿæ%ãã—èf½ãSãã, ã, <ã”ã”ã, ’èã~ã—ã|ã,,ã¼ãã™ã€,
ã”ã®ã, çãf%ããfã, mã, ¶ãfãSèª-æ~Žã•ã, CEã|ã,,ã, <è,,tã¼±æ€Sã®æ, aç””ã«é-çã™ã, <ã
Cisco PSIRTã«ã”,,ã>ã,%ã, CEã|ã,,ã¼ãã>ã,,ã€,

ã†°ã...,

ã, .ã, 1ã, 3ã ¯ã€ã"ã®è,,†ã¼±æ€šã,'ç™ºè|ã—ã€ã±ãšã—ã|ã,,ãÿãã,,ãÿMnemo
Marstranderæ°ã"Alvaro Gutierrezæ°ããšã,^ã³Matteo
Malvicaæ°ã«æ,,ÿè-ã,,ãÿã—ã¼ã™ã€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sni-data-exfil-mFgzXqLN>

æ''è'',ã±ÿæ'

ãfãf¼ã,,ãfsãf³	èª-æ
1.1	è,,†ã¼±æ€šãã½±éÿçã,'ã—ã'ã,«è£½ã"ãããšã,^ã³ã¯èf½æ€šã®ã
1.0	ã^ãžã...-é-ãfãfãf¼ã,¹

ã^©ç''è|ç',,

æœ-ã,çãf%ãfã,ãã,¶ãfãç,,jäçè"¼ã®ã,,ã®ã"ã—ã|ã"æãã¼ã—ã|ãšã,šã€
æœ-ã,çãf%ãfã,ãã,¶ãfã®æf...ã±ãšã,^ã³ãfãfã,ã®ã½çç"ã«é-çã™ã,«è²-ã»ã®ã,€
ã¼ãÿã€ã,ã,¹ã,³ã¯æœ-ãf%ã,ãfãfãfãfã®ã†...ã®¹ã,'ã^ãšããã—ã«ã%æ'ã—ã€
æœ-ã,çãf%ãfã,ãã,¶ãfã®è"~è:°ã†...ã®¹ã«é-çã—ã|æf...ã±é...ãçjã® URL
ã,çœçç•ÿã—ã€ãçç<ã®è»çè¼%ã,,æ,,è"³ã,'æ-½ã—ãÿã'ã^ã€ã½"ç³¼ã€ççççç
ã"ã®ãf%ã,ãfãfãfãfã®æf...ã±ã¯ã€ã,ã,¹ã,³è£½ã"ã®ã,"ãfãf%ãf!ãf¼ã,¶ã,'ã³¼è±j

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。