

ã,·ã,¹ã,³è£1/2å“◊ã◊«å½±éÿ¿ã◊™ã,ãf-ã,ãfã2ãf



ã,çãf%ãf◊ã,ã,¶ã,¶ãfããf¼ID : cisco-sa-
YU855201-J3z8CKTX

[CVE-2021-27862](#)

ã^◊ã...-é-ã—¥ : 2022-09-27 16:00

[CVE-2021-](#)

æœ€œæ>æ-°æ—¥ : 2022-10-05 18:16

[27861](#)

ãf◊ãf¼ã,ãfšãf³ 1.1 : Final

[CVE-2021-](#)

CVSSã,¹ã,³ã,ç : 4.7

[27853](#)

ã>žé◊¿ç- : Yes

[CVE-2021-](#)

Cisco ãf◊ã,° ID : [CSCvw92154](#) [CSCwa09081](#)

[27854](#)

[CSCwa14271](#) [CSCwa14282](#) [CSCwa18310](#)

[CSCvw99743](#) [CSCvx33758](#) [CSCwa18093](#)

[CSCwa01097](#) [CSCwa06265](#) [CSCwa06145](#)

[CSCvz88705](#) [CSCvx35085](#) [CSCvz89602](#)

[CSCwa18209](#) [CSCwa14950](#) [CSCwa14942](#)

[CSCvx35087](#) [CSCvx37987](#) [CSCvz91291](#)

[CSCwb01481](#) [CSCvz96133](#) [CSCwa04809](#)

æ—¥æœ-èªžã◊«ã,^ã,ãæf...å ±ã◊-ã€◊è±èªžã◊«ã,^ã,ãžÿæ-ãã◊®é◊žã...-å¼◊ã◊

æ!,è!◊

2022å¹9æœ^27æ—¥ã◊«ã€◊Cert/CCã◊CEVU855201ã◊®ã,€éí"ã◊"ã◊—ã◊|ã,ã,¹ã,³è£1/2å"ã◊«å½±
[0ã,¹ã,¿ãffã,ãf³ã,°ã◊šã,^ã◊³/ã◊³¼ã◊ÿã◊-802.3ãf~ãffãf€ãf¼ã,'ã½¿ç""ã◊—ã◊|ãf◊ã,ããfã,¹ã◊šã◊](#)

- CVE-2021-27853:VLAN

0ãf~ãffãf€ãf¼ã◊"LLC/SNAPãf~ãffãf€ãf¼ã◊®çµ,,ã◊¿ã◊^ã,ã◊ã◊>ã,'ã½¿ç""ã◊—ã◊|ã€◊IPv6
RAã,-ãf¼ãf%ãã,,,ARPã,ããf³ã,¹ãfšã,ã,ãfšãf³ã◊ã◊©ã◊®ãf-ã,ããfã2ãf◊ãffãf^ãfãf¼ã,ãfã,£ãfã,£ã

- CVE-2021-27854:VLAN

0ãf~ãffãf€ãf¼ã◊ã,ããf¼ã,µãf◊ãffãf^ã◊ã,%,WiFia◊,ã◊®ãfãf-ãf¼ãfãã%ã◊>ã◊šã◊®LLC
RAã,-ãf¼ãf%ãã◊ã◊©ã◊®ãf-ã,ããfã2ãf◊ãffãf^ãfãf¼ã,ãfã,£ãfã«ã,¿ãfãf³ã,°æ©ÿèf½ã,'ãf◊ã

- CVE-2021-

27861i¼šç,,ãš¹ã◊ãé·ã◊ã◊®LLC/SNAPãf~ãffãf€ãf¼ãi¼^ã◊šã,^ã◊³ã,ããf—ã,ããfšãf³ã◊šVLAN0ãã
RAã,-ãf¼ãf%ãã◊ã◊©ã◊®ãf-ã,ããfã2ãf◊ãffãf^ãfãf¼ã,ãfã,£ãfã«ã,¿ãfãf³ã,°æ©ÿèf½ã,'ãf◊ã

- CVE-2021-27862:IPv6

RAã,-ãf¼ãf%ãã◊ã◊©ã◊®ãf-ã,ããfã2ãf◊ãffãf^ãfãf¼ã,ãfã,£ãfã«ã,¿ãfãf³ã,°æ©ÿèf½ã◊-ã€◊

ã◊"ã,£ã,%,ãã◊®è,,†å½±æ€šã◊£ã,◊æ£ã^©ç""ã◊ã,£ã,ãã◊"ã€◊és£æžÿã◊™ã,ãæ"»æ'fè€...ã◊£è

L2ãf~ãf©ãf³ã,¹ãf◆ãf¼ãf^ã,µãf¼ãf"ã,¹ã◆Çè"ã@šã◆•ã,Çã◆ÿIOS XRãf«ãf¼ã,¿	CSCvz88705 CSCvz89602	ä¿@æfæ,^ã◆¿ã,¼
MS390	N/A	ãf€ã,µãfŠãfÿãfj
MS210	N/A	ä¿@æfæ,^ã◆¿ã,¼
MS225		
MS250		
MS350		
MS355		
MS410		
MS420		
MS425		
MS450		
Nexus 3000 ã,·ãf^ãf¼ã,°ã,¹ã,µãffãf◆	CSCvx33758	ä¿@æfæ,^ã◆¿ã,¼
Nexus 5500 ãf—ãf©ãffãf^ãf•ã,©ãf¼ãf ã,¹ã,µãffãf◆	CSCvx35087	ä¿@æfæ,^ã◆¿ã,¼
Nexus 5600 ãf—ãf©ãffãf^ãf•ã,©ãf¼ãf ã,¹ã,µãffãf◆		
Nexus 6000 ã,·ãf^ãf¼ã,°ã,¹ã,µãffãf◆		
Nexus 7000 ã,·ãf^ãf¼ã,°ã,¹ã,µãffãf◆	CSCvx35085	ä¿@æfæ,^ã◆¿ã,¼
Nexus 9000ã,·ãf^ãf¼ã,°ã,¹ã,µãffãf◆¼ã^¹ã,¿ãf³ãf%ã,Çãfãf³ãfÇãf¼ãf%ãoi¼%ã	CSCvx33758	ä¿@æfæ,^ã◆¿ã,¼
250 ã,·ãf^ãf¼ã,°ã,¹ãfžãf¼ãf^ã,¹ã,µãffãf◆	CSCvw92154	ä¿@æfæ,^ã◆¿ã,¼
350 ã,·ãf^ãf¼ã,°ãfžãf◆ãf¼ã,ãf%ã,¹ã,µãffãf◆		
350X ã,·ãf^ãf¼ã,°ã,¹ã,¿ãffã,«ãf—ãf«ãfžãf◆ãf¼ã,ãf%ã,¹ã,µãffãf◆		
550X ã,·ãf^ãf¼ã,°ã,¹ã,¿ãffã,«ãf—ãf«ãfžãf◆ãf¼ã,ãf%ã,¹ã,µãffãf◆		
Business 250 ã,·ãf^ãf¼ã,°ã,¹ãfžãf¼ãf^ã,¹ã,µãffãf◆		
Business 350 ã,·ãf^ãf¼ã,°ãfžãf◆ãf¼ã,ãf%ã,¹ã,µãffãf◆		

CVE-2021-27854

Ciscoã,çã,¬ã,»ã,¹ãf◆ã,µãf³ãf^

ã,·ã,¹ã,³ã◆¬ã€ã,ã,¹ã,³ã,Çã,¬ã,»ã,¹ãf◆ã,µãf³ãf^ã◆«è"ã@šã◆•ã,Çã◆|ã◆,,ã,«FHSæ©ÿèf½ã◆«ã¬³

ã,·ã,¹ã,³ã◆®ã,Çã,¬ã,»ã,¹ãf◆ã,µãf³ãf^ã◆,ã◆®ã½±éÿ¿ã◆«é-Çã◆™ã,«èªæÿ»ã◆®ã,€ç'ã◆"ã◆—ã◆

[Access Points VLAN Bypass from Native VLAN](#)

[Vulnerabilityã◆Çãå...-é-ã◆•ã,Çã◆¾ã◆—ã◆ÿã€,](#)

CVE-2021-27861

æ¬;ã®è;ã«ã€CVE-2021-

27861ãšè¬æžã•ã,Œã|ã,,ã,è,,tä¼±æ€šã®ã½±éÿã,ã—ã'ã,ã,ã,1ã,³è£½ã"ã,'çªã

æ³'¼šã,ãfãf¼ãf^çµ,ã°tè£½ã"ããè©•ã¾;ã•ã,Œã|ã,,ã¾ãã,ã,"ã€,

ã,ã,1ã,³è£½ã"	Cisco Bug ID	
Cisco IOSã,½ãfãf^ã,ã,šã,ç¼¼šã,1ã,ªãffãf		
Catalyst 6500ãšã,ã³ 6800ã,ãfãf¼ã,ã,1ã,ªãffãf	CSCwa06265	ã;®æ£æ,ãã,½
Catalystãfã,ã,ã,ãf«ãf«ãfã,£ãf³ã,ã,ãfãf¼ã,ã,1ã,ªãffãf	CSCwa14950	ã;®æ£æ,ãã,½
ãfã,ã,ãfã,1ã,ªãffãf	CSCwa14282	ã;®æ£æ,ãã,½
Cisco IOS XRã,½ãfãf^ã,ã,šã,ç		
L2ãfãf©ãf³ã,1ãfãf¼ãf^ã,µãf¼ãf^ã,1ããè"ãšã•ã,ŒãÿIOS XRãfãf¼ã,ç	CSCwa04809	ã;®æ£æ,ãã,½
Cisco Merakiã,1ã,ªãffãf		
MS210 MS225 MS250 MS350 MS355 MS410 MS420 MS425 MS450	N/A	ã;®æ£æ,ãã,½
Cisco NX-OSã,½ãfãf^ã,ã,šã,ç		
Nexus 3000ã,ãfãf¼ã,ã,1ã,ªãffãf	CSCwa01097	ã;®æ£æ,ãã,½
Nexus 5500ãf—ãf©ãffãf^ãfã,©ãf¼ãfã,1ã,ªãffãf		
Nexus 5600ãf—ãf©ãffãf^ãfã,©ãf¼ãfã,1ã,ªãffãf	CSCwa18209	ã;®æ£æ,ãã,½
Nexus 6000ã,ãfãf¼ã,ã,1ã,ªãffãf		
Nexus 7000ã,ãfãf¼ã,ã,1ã,ªãffãf	CSCwa18310	ã;®æ£æ,ãã,½
Nexus 9000ã,ãfãf¼ã,ã,1ã,ªãffãfã¼ã,1ã,çãf³ãf%ã,çãfãf³ãfçãf¼ãf%ã¼ã	CSCwa01097	ã;®æ£æ,ãã,½
Cisco Small Businessã,1ã,ªãffãf		
250ã,ãfãf¼ã,ã,1ãfãf¼ãf^ã,1ã,ªãffãf	CSCwa09081	ã;®æ£æ,ãã,½

350 ā, ·āf ^a āf ¹ / ₄ ā, ° āfžāf āf ¹ / ₄ ā, āf% ā, ¹ ā, pāffāf		
350X ā, ·āf ^a āf ¹ / ₄ ā, ° ā, ¹ ā, ĭāffā, «āf-āf« āfžāf āf ¹ / ₄ ā, āf% ā, ¹ ā, pāffāf		
550X ā, ·āf ^a āf ¹ / ₄ ā, ° ā, ¹ ā, ĭāffā, «āf-āf« āfžāf āf ¹ / ₄ ā, āf% ā, ¹ ā, pāffāf		
Business 250 ā, ·āf ^a āf ¹ / ₄ ā, ° ā, ¹ āfžāf ¹ / ₄ ā [^] ā, ¹ ā, pāffāf		
Business 350 ā, ·āf ^a āf ¹ / ₄ ā, ° āfžāf āf ¹ / ₄ ā, āf% ā, ¹ ā, pāffāf		

CVE-2021-27862

ā, ·ā, ¹ā, ³ā -ā€ā, ·ā, ¹ā, ³ā, ĭā, -ā, »ā, ¹āf ā, pāf³āf[^]ā «è ¨ ā@šā ·ā, Ćā | ā, ā, <FHSæ©ÿèf¹/₂ā «ā⁻ā
 è, †ā¹/₄±æ€šā, 'ā «ā, "ā šā, ā^aā, ā "ā "ā Ćçç^oè^a ā ·ā, Ćā ÿèf¹/₂ā"
 ā "ā @ā, ĭāf%āf ā, pā, ¶āf^aā @. †ā¹/₄±æ€šā @ā, ā, <èf¹/₂ā" ā, »ā, -ā, āfšāf³ā «è ¨ è¹/₄%ā ·ā

CVE-2021-27853

ā, ·ā, ¹ā, ³ā -ā€ā "ā @è, †ā¹/₄±æ€šā Ćā»¥ā, ā @ā, ·ā, ¹ā, ³èf¹/₂ā" ā «ā -ā¹/₂±éÿā, ä, Žā[^]ā

ONTā, ¹ā, pāffāf

- Catalyst PONā, ·āf^aāf¹/₄ā, °ā, ¹ā, pāffāf

IOSā, ¹ā, pāffāf

- Catalyst 1000 ā, ·āf^aāf¹/₄ā, ° ā, ¹ā, pāffāf

IOS XEāf-āf©āffāf[^]āf·ā, ©āf¹/₄āf

- Catalyst 8000 ā, ·āf^aāf¹/₄ā, ° ā, ¨āffā, āf-āf©āffāf[^]āf·ā, ©āf¹/₄āf

NX-OS ā, ¹/₂āf·āf[^]ā, ¹ā, šā, ĭ

- MDS 9000 ā, ·āf^aāf¹/₄ā, ° āfžāf«āf āf-ā, pāf ā, ¹ā, pāffāf
- Nexus 1000V ā, ·āf^aāf¹/₄ā, ° ā, ¹ā, pāffāf
- Nexus 9000 ā, ·āf^aāf¹/₄ā, ° āf·ā, ĭāf-āf^aāffā, -ā, ¹ā, pāffāf i[^]ā, ĭāf-āfā, ±āf¹/₄ā, ·āfšāf³ ā, »āf³āf[^]āfāffā, -ā, pāf³āf·āf©ā, ¹āf[^]āf©ā, -āf āfEi¹/₄[^]ACIi¹/₄%āfĭāf%oi¹/₄%
- UCS 6x00ā, ·āf^aāf¹/₄ā, °āf·ā, ĭāf-āf^aāffā, -ā, pāf³ā, ĭāf¹/₄ā, ³āf ā, -āf[^]

Merakiā, ¹ā, pāffāf

- GS110ā, ¹ā, pāffāf
- MS22ā, ¹ā, pāffāf
- MS42ā, ¹ā, pāffāf
- MS120ā, ¹ā, pāffāf

- MS125ã, 1ã, ðãffãf
- MS220ã, 1ã, ðãffãf
- MS320ã, 1ã, ðãffãf

CVE-2021-27854

ã, ·ã, 1ã, 3ã ¯ã€ã"ã®è,,†ã¼±æ€šã«Eä»¥ä,ã®ã,ã,1ã,3è£½ã"ã«ã¯ã½±éÿ;ã,'ä,Žã^ã

- ã, çã, ¯ã, »ã, 1ãfã, ðãf³ãf^
- AireOSã, çã, ¯ã, »ã, 1ãfã, ðãf³ãf^
- Merakiã, çã, ¯ã, »ã, 1ãfã, ðãf³ãf^

CVE-2021-27861

ã, ·ã, 1ã, 3ã ¯ã€ã"ã®è,,†ã¼±æ€šã«Eä»¥ä,ã®ã,ã,1ã,3è£½ã"ã«ã¯ã½±éÿ;ã,'ä,Žã^ã

ONTã, 1ã, ðãffãf

- Catalyst PONã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf

IOSã, 1ã, ðãffãf

- Catalyst 1000ã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf
- ç'£æ¥ç"ã, ðãf¼ã, ðãffãfã, 1ã, ðãffãf

IOS XEãfãf¼ã, ç

- IOS XEãfãf¼ã, ç¼ã, ðãf¼ã, ðãffãf^ã»®æf³ã»žç·šãšè"ã®šãã, Eã|ã,,ã,ã'ã^¼%o

IOS XEã, ½ãfãf^ã, 1ã, šã, çã, 1ã, ðãffãf

- Catalyst 3650ã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf
- Catalyst 3850ã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf
- Catalyst 4500Eãšã, ^ã³4500Xã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf
- Catalyst 9000ã, ·ãf³ãf¼ã, °ã, 1ã, ðãffãf

Merakiã, 1ã, ðãffãf

- GS110ã, 1ã, ðãffãf
- MS22ã, 1ã, ðãffãf
- MS42ã, 1ã, ðãffãf
- MS120ã, 1ã, ðãffãf
- MS125ã, 1ã, ðãffãf

- MS220ã, 1ã, ðãffãf
- MS320ã, 1ã, ðãffãf
- MS390ã, 1ã, ðãffãf

NX-OS ã, 1/2ãf•ãf^ã, 1ã, §ã, ç

- MDS 9000 ã, ðãfãf1/4ã, °ãfžãf«ãfãf-ã, ðãfã ã, 1ã, ðãffãf
- Nexus 1000V ã, ðãfãf1/4ã, °ã, 1ã, ðãffãf
- Nexus 9000 ã, ðãfãf1/4ã, °ãf•ã, ;ãf-ãfãffã, -ã, 1ã, ðãffãf i1/4ã, çãf—ãfã, ±ãf1/4ã, ðãfãf³ã, »ãf³ãf^ãfãffã, -ã, ðãf³ãf•ãf©ã, 1ãf^ãf©ã, -ãfãf£i1/4^ACIi1/4%ãfçãf1/4ãf%oi1/4%ã
- UCS 6x00ã, ðãfãf1/4ã, °ãf•ã, ;ãf-ãfãffã, -ã, ðãf³ã, çãf1/4ã, ³ãfã, -ãf^

CVE-2021-27862

ã, ðã, 1ã, ³ã -ã€ã"ã@è,, tã1/4±æ€Sã€€ã»¥ã, çã, ðã, ðã, 1ã, ³è£1/2ã"ã«ã-ã1/2±éY;ã, 'ã, žã^ã

- ã, çã, -ã, »ã, 1ãfã, ðãf³ãf^
- AireOSã, çã, -ã, »ã, 1ãfã, ðãf³ãf^
- Merakiã, çã, -ã, »ã, 1ãfã, ðãf³ãf^

è©³ç°

ã"ã, €ã, %ã@è,, tã1/4±æ€Sã-ã3ã~é-çãç, ã«ã-ãªããã€ã,, ãšã, €ã<ã@è,, tã1/4±æ

CVE-2021-27853

èçã•ã@ã, ðã, 1ã, ³è£1/2ã"ã@ã, 1ã, çãffã, -ã, ðã, €ãYã, ðãf1/4ã, ðãfãf^ã, çã, °ãf~ãffãf€ãf1/4ã@ã

ã"ã@è,, tã1/4±æ€Sã-ã€ã, šã1/2ã±ãf—ãfãf^ã, ³ãf«ã€ãf-ã, ðãf³ã

FHSæ©Yèf1/2ã, 'èµã•ã™ã, <ã, ^ãtã«æ±ã@šãšãããªã,, á^ã«ã€ãf•ãf-ãf1/4ãfã, 'è»ç

ã, ðã, 1ã, ³ãšã-ã€æœ-è,, tã1/4±æ€Sã«ã³ã‡|ã™ã, <ã, 1/2ãf•ãf^ã, |ã, šã, ç

ã, çãffãf—ãfãf1/4ãf^ã, 'ãfãfãf1/4ã, 1ã—ã|ã,, ã³ãã>ã, "ã€, æœ-è,, tã1/4±æ€Sã«ã³ã‡|ã™ã, çã

CVE IDi1/4šCVE-2021-27853

ã, »ã, ðãf¥ãfãf^ã, £ã1/2±éYçè©•ã3/4ji1/4^SIRi1/4%oi1/4šã,

CVSS ãf™ãf1/4ã, 1ã, 1ã, ³ã, çã1/4š4.7

CVSSãf™ã, -ãf^ãf<i1/4šCVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVE-2021-27853i1/4šèç1/2ãŠ è©³ç°

IEEE Std 802.1Q-

2018æ™æ°ã«ã-ã€ãf—ãf©ã, ðã, °ãfãftã, £æf...ã ±ã, 'ã1/4€ã€ã™ã, <ã, çã, °ãf~ãffãf€ãf1/4ã, 'æ€ã

IDã0ã«è"ã@šãã, €ã€€é€šã,, ãé€ãç;ã...fMACã, çãf%ãf-ã, 1ã "Ethertype/sizeãf•ã, £ãf1/4ãf<

VLANā,ġā,®āf³ā,°āĈEä½ġç"ā•ā,ĈEā,āfāffāfāfāfāfā,āšāāā€éšā,ā€éäġā...fMACā,
802.1ADā«āā°ĈEé†ā,ġā,®āf³ā,°āĈEāā,ā,šā€é€äġā...fMACā,čāf%āāf-ā,¹ā Ethertype/siz
TAGāfāffāf€āf¼ā C-TAGāfāffāf€āf¼āĈEā«ā¼ā,ĈEā|ā,,ā¼ā™ā€,

IEEEæ™æ°-802.1Q-

2018āšāā,ġā,°ā®æ°āĈE2āā¼āšāè|āā®šāā,ĈEā|ā,,ā¼āā,“āĈEāāā
āfāf-āf¼āf ā,ā—āġā™ā,āæ-ġā®āf†āfā,ā,ā,¹ā®ā®ÿèĒ...ā«āġœāā~ā|ā€āfāf-āf¼āf

CVE-2021-27853: Cisco Network Operating Systems

ā“ā®ā,»ā,ā,āfšāf³āšāā€ā½±éÿġā,ā—āā,āā•ā¼āā¼āCiscoāfāffāfāfāfāfā
ID
0ā,ġā,°ā,āĈEāā,āāf¼ā,μāfāffāfāfāf-āf¼āf ā,ā†|ç†ā™ā,āæ-¹æ³ā«āāā,,ā|ā...ā½

Cisco IOSā,½āfāfā,ā,šā,ĉ¼šā,¹ā,āffāfāf

āf†āfā,©āf«āfāšāā€è²ā½ā™ā,ā™ā¹ā|ā®Cisco
IOSā,¹ā,āffāfāfāā€VLAN ID
0ā,ġā,°ā,ā,ā«ā,āfāf-āf¼āf āfāffāf€āf¼ā,āĈEāāç€āġāfā,±āffāfā,ā†|ç†ā—ā¼ā™ā
æ³¼šā,μfāf¼āfāĈEçμ,ā†ā—āÿCisco IOSā,¹ā,āffāfāfāā€Cisco Product Security
Incident Response Team(PSIRT)ā«ā,ā,è©ā¼ā,ā—āā|ā,,ā¼āā,“ā€,

Cisco IOS XEā,½āfāfā,ā,šā,ĉ¼šā,¹ā,āffāfāf

āf†āfā,©āf«āfāšāā€Cisco Catalyst 4500Eā,āfāf¼ā,°ā,¹ā,āffāfāfāā€VLAN ID
0ā,ġā,°ā,ā,ā«ā,āfāf-āf¼āf āfāffāf€āf¼ā,āĈEāāç€āġāfā,±āffāfā,ā†|ç†ā—ā¼ā™ā
Cisco IOS XEā,¹ā,āffāfāfāā®āf†āfā,©āf«āfā®ā•ā½œāšāā€VLAN ID
0ā,ġā,°ā,ā,ā«ā,āfāf-āf¼āf āfāffāf€āf¼ā,āĈEāāā™ā¹ā|ā®āfāf©āfā,āĈEāf
ID 0ā,ġā,°ā,āĈEāā,āfāf-āf¼āf ā®āġā,ā†|ç†ā—ā¼ā™ā€,

```
switchport voice vlan dot1p
```

Cisco IOS XEā,½āfāfā,ā,šā,ĉ¼šāfāf¼ā,ġ

ā,μf¼āf“ā,¹ā,āf³ā,¹ā,ġāf³ā,¹āĈEèā®šāā,ĈEāÿCisco IOS
XEāf†āfāā,ā,¹āā€èā®šā«ā¼āāĒā|VLAN ID
0ā,ġā,°ā,ā†|ç†ā—ā¼ā™ā€,VLANāf™āf¼ā,¹ā®ā,μāf¼āf“ā,¹ā®āāā€æœ€ā,šā½ā

encapsulation dot1q priority-tagged

exact

default

VLAN ID

0

any

Cisco IOS XR

IOS

XR

ID

encapsulation dot1q priority-tagged exact

default

Cisco NX-OS

VLAN ID

ID

Cisco Small Business

Cisco Small Business

VLAN ID

CVE-2021-27854

CVE-2021-

27854

ã,ã,1ã,3ã

CVE ID: CVE-2021-27854

ã,»ã,ãf¥ãfãfãfã,£ã½±éÿ¿è©•ã¾¼;ï¼^SIRi¼%oi¼šä,

CVSS ãf™ãf¼ã,¹ã,¹ã,³ã,ç¼¼š4.7

CVSSãf™ã,¬ãf^ãf«i¼šCVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVE-2021-27861

è©²ã½“ã™ã,«ã,¬ã,¹ã,³è£½ã”ã@ã,ããf¼ã,µãfãffãf^ã±|çãtã«ãšãã,«è,,tã¼±æ£šã«ã,^ã,šã€

ã“ã@è,,tã¼±æ£šã¬ã€SNAP/LLCã,ããf¼ã,µãfãffãf^ãfãf¬ãf¼ãfã@ä,ããããã^tãªæªœè

ã,ã,¹ã,³ãšã¬ã€æœ¬è,,tã¼±æ£šã«ã¾ã±|ã™ã,ã,½ãfãf^ã,|ã,šã,ç

ã,çãffãf¬ãfãf¼ãf^ã,ãfããfãf¼ã,¹ã—ã|ã,,ã¾ãã>ã,“ã€ã,€éfã@è£½ã”ãšã¬ã€ã

CVE ID¼šCVE-2021-27861

ã,»ã,ãf¥ãfãfãfã,£ã½±éÿ¿è©•ã¾¼;ï¼^SIRi¼%oi¼šä,

CVSS ãf™ãf¼ã,¹ã,¹ã,³ã,ç¼¼š4.7

CVSSãf™ã,¬ãf^ãf«i¼šCVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVE-2021-27861: Cisco Network Operating Systems

ã“ã@ã,»ã,¬ã,ãfšãf³ãšã¬ã€ã½±éÿ¿ã,ã—ã^ã,ããã¾ã¬ã¾ãªCiscoãffãf^ãfã

Cisco IOSã,½ãfãf^ã,|ã,šã,ç¼¼šã,¹ã,ããfãfã

è©²ã½“ã™ã,«Cisco

IOSã,½ãfãf^ã,|ã,šã,çè£½ã”ã¬ã€è¿½ãšã@FHSæ©ÿèf½æªœæÿ»ã,è;CEã,ãšã«SNAP/LLC

Cisco IOS XRã,½ãfãf^ã,|ã,šã,ç

è©²ã½“ã™ã,«Cisco IOS

XRã,½ãfãf^ã,|ã,šã,çè£½ã”ã¬ã€è¿½ãšã@FHSæ©ÿèf½æªœæÿ»ã,è;CEã,ãšã«SNAP/LLC

Cisco NX-OSã,½ãfãf^ã,|ã,šã,ç

è©²ã½“ã™ã,«Cisco NX-

OSã,½ãfãf^ã,|ã,šã,çè£½ã”ã¬ã€è¿½ãšã@FHSæ©ÿèf½æªœæÿ»ã,è;CEã,ãšã«SNAP/LLC

Cisco Small Businessã,¹ã,ããfãfã

è©²ã½“ã™ã,«Cisco Small

Businessã,¹ã,ããfãfããšã¬ã€æœ€ãª\$1,500ã@é•ããfã,£ãf¼ãf«ãf%ã,æCEãªSNAP/LLC

¼ž

1,535ã@é•ãã@SNAP/LLCãfãf¬ãf¼ãfã¬ã€è¿½ãšã@FHSæ©ÿèf½ã,ããfã,¹ãfšã,¬ã,ãfšãf

CVE-2021-27862

CVE-2021-

27862ã Sã ã€ ãf•ãf-ãf¼ãf ã CE802.3ã <ã,%00802.11ã «ã%00æ >ã •ã,CEã,<æ-¹æ³•ã é•ã
ã,ã,¹ã,³ã ã€ ã ã,CEã,%00ã @ãf•ãf-ãf¼ãf ã%00æ >ã,ã†|ç ã™ã,<és>ã «ã€ ãf-ã,ããfããf-ã,¹ã

CVE IDi¼š CVE-2021-27862

ã,»ã,ãfãfãfãfãfã,£ã½±éÿçè©•ã³¼;í¼^SIRi¼%oi¼šã,
CVSS ãf™ãf¼ã,¹ã,¹ã,³ã,ç¼¼š4.7
CVSSãf™ã,ãf^ãf<¼¼š CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

ã>žé ç-

ã ã,CEã,%00ã @è,,ã¼±æ€šã @ã,€éf ã «ã³¼ã†|ã™ã,<ã>žé ç-ã CEã ã,šã ¼ã™ã€,

CVE-2021-27853

ç@;ç ã€...ã ã€ ãf-ã,ããfãã2ã,çã,ã,»ã,¹ã,³ã³ãf^ãfãf¼ãf«ãfã,¹ãf^ (ACL)ã,'ã½çç"ã —ã | ethertyp
FHSã CEè ã@šã •ã,CEã |ã,,ã,<ã,çã,ã,»ã,¹ãf ãf¼ãf^ã «ã@ÿè£...ã šã ã,ãf-ã,ããfãã2
ACLã @ã¼ã,æ-ãã «çãã —ã ¼ã™ã€,

Cisco IOSã,¼ãf•ãf^ã,ã,šã,ç¼¼šã,¹ã,ããffãf

```
!  
mac access-list extended CSCwa14271  
  permit any any 0x86DD 0x0  
  permit any any 0x800 0x0  
  permit any any 0x806 0x0  
  deny any any  
!  
interface GigabitEthernet1/0/1  
  switchport access vlan 5  
  switchport voice vlan dot1p  
  ipv6 nd raguard attach-policy HOSTS  
  mac access-group CSCwa14271 in  
!
```

Cisco IOS XEã,¼ãf•ãf^ã,ã,šã,ç¼¼šã,¹ã,ããffãf

ã,¹ã,ããffãf ã,šã @Cisco IOS XEã,¼ãf•ãf^ã,ã,šã,çã šã ã€ Cisco
IOSã,¼ãf•ãf^ã,ã,šã,çãfãfãfãf¼ã,¹7.6.1ã »é™ ã€ ã ãÿã ã —æœ€ã^ ã @ãç@æfæ,^ã çãfãã
5ã «ã,çã,ã,»ã,¹ãf ãf¼ãf^ã CEã ã,ã,ã'ã ^ã€ ã ã"ã @ã •é;CEã ã interface vlan
5ã CEè ã@šã •ã,CEã |ã,,ãããã,,ã'ã ^ã€ «ã @ã çç™ç"ÿã —ã ¼ã™ã€ Cisco
IOSã,¼ãf•ãf^ã,ã,šã,çã @è,,ã¼±ã ããfããfãf¼ã,¹ã «ã³¼ã —ã ã |ã "ã @ã •é;CEã,'è»½æ,ã™ã

!

Cisco Small Business, 1a, paffaf

è»1/2æ, >æZç1/2@ã,,å>žé çç-ã-ã,ã,Šã 3/4ã>ã,“ã€,

ã“ã,CEã,%oã@ã>žé çç-ã-ã°Žã...¥ã•ã,CEã|ãŠã,Šã€ãftã,1ãf^ç°ãçfãŠã-ã@ÿè“1/4æ,^ã

ä; @æfxæ, ^ã çã, 1/2ãf•ãf^ã, |ã, Šã, ç

[ã.1/2ãf•ãf^ã.lã.Šã.çã@ã,çãffãf—ã,°ãf-ãf1/4ãf%ã, 'æœœè“Žã™ã, <és>ã«ã-ã€ã.ã.1ã.3](#)

[ã.>ã.ãf¥ãfãfãfã.£ã.çãf%ãfã,ã,ã,¶ã,¶ãfã](#)

[ãfšãf1/4ã,ãŠã...¥æ%ãŠãã,ã,ã,ã,1ã,3è£1/2ã”ã@ã,çãf%ããfã,ã,ã,¶ã,¶ãfã,ã@šæœÿçš,ã«ãç](#)

ã,1/2ãfãf¥ãf1/4ã,ãfšãfã,ã€1/4ã,çç°èãã—ã|ããããã•ãã,ã€,

ã,ãšã,CEã@ã'ã^ã,,ã€ã,çãffãf—ã,°ãf-ãf1/4ãf%ã™ã,ãfãfãã,ã,ã,1ãã«ããã^tããfjãfçã

Technical Assistance

Centeri1/4^TACi1/4%ã,,ã—ããã-ã¥ç',ã—ã|ã,,ã,ãfjãfãfãfãfãfã,1ãf—ããfã,ããfãf1/4ã

ä; @æfxæ, ^ã çãfãfãfãf1/4ã, 1

CVE-2021-27853

ç™œè;CEã™,ç,1ãšã-ã€æ-jã@èi“ã«çœã™ãfãfãfãf1/4ã,1æf...ã±ã-æ£çç°ãšã—ãÿã€,ã

IDã@è©3ç°ã,»ã,ã,ãfšãfã,ã,ã,ç...šã—ã|ããããã•ãã,,ã€,

è£1/2ã“	Cisco Bug ID	First Fixed Releasei1/4ä; @æfxæã,ã,CEãÿæœœã^ã@ãfãfãfãf1/4ã,1i1/4%
Cisco IOS XEã,1ã,ã,ãfãfãfãf	CSCvz91291	17.6.3 17.8.1

CVE-2021-27854

ã,ã,1ã,3ã-ã€ã,çã,ã,»ã,1ãfã,ããfãfã«è“ãšãã,ã,CEãÿFHSæ©ÿèf1/2ã«ã3/4ã™ã,ã1/2±èÿã

CVE-2021-27861

ã“ã@ãf%ã,ãf¥ãfãfãfãfã@ç™œè;CEã™,ç,1ãšã-ã€ã,ã,1ã,3ã-ã,ã,1ã,3è£1/2ã”ã«ã3/4ã™

CVE-2021-27862

ã,ã,1ã,3ã-ã€ã,çã,ã,»ã,1ãfã,ããfãfã«è“ãšãã,ã,CEãÿFHSæ©ÿèf1/2ã«ã3/4ã™ã,ã1/2±èÿã

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。