

Cisco SD-WAN vManage

High severity vulnerability in Cisco SD-WAN vManage



Cisco Security Advisory ID : cisco-sa-

[CVE-2022-](#)

vmanage-msg-serv-AqTup7vs

[20696](#)

Published : 2022-09-07 16:00

Last Updated : 2022-09-27 21:40

Version : 1.2 : Final

CVSS Score : [7.5](#)

Impact : Yes

Cisco ID : [CSCvx87376](#)

High severity vulnerability in Cisco SD-WAN vManage

Summary

Cisco SD-WAN vManage

A high severity vulnerability was discovered in Cisco SD-WAN vManage. The vulnerability is located in the vmanage-msg-serv-AqTup7vs service. The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5. The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

The vulnerability is located in the vmanage-msg-serv-AqTup7vs service. The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

The vulnerability is rated as High severity with a CVSS score of 7.5.

The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs>

References

High severity vulnerability in Cisco SD-WAN vManage

The vulnerability is caused by a buffer overflow in the vmanage-msg-serv-AqTup7vs service. The vulnerability is identified as CVE-2022-20696. The vulnerability is rated as High severity with a CVSS score of 7.5.

Cisco SD-WAN vManage

ã,½ãf•ãf^ã,|ã,šã,ćãfããfããf¼ã,¹ã,'ã@ÿè|Ĉã—ã|ã,,ã,ã'ã^ãšã™ã€,

è,,†ã¼±æ€šãĈã~ãœ"ã™ã,ć Cisco

ã,½ãf•ãf^ã,|ã,šã,ćãfããfããf¼ã,¹ã«ã»ã»ã,,ã|ã-ã€ãã"ã®ã,ćãf%ããfãã,ãã,¶ãfãã®ã€Ĉã

è,,†ã¼±æ€šã,'ã«ã,"ãšã,,ãªã,,ã"ã"ã"ãĈçç°èªãã•ã,Ĉãÿè£½ã"

ã"ã®ã,ćãf%ããfãã,ãã,¶ãfãã®ã€,,†ã¼±æ€šã®ã,ã,è£½ã"ã,»ã,ã,ãfšãf³ã«è~è¼%ãã•ã

ã,ã,¹ã,³ã-ã€ãã"ã®è,,†ã¼±æ€šãĈã»ã,ããã,ã,¹ã,³è£½ã"ã«ã-ã½±éÿã,ã,žã^ã

- IOS XE SD-WAN ã,½ãf•ãf^ã,|ã,šã,ć
- SD-WAN vBond Orchestrator ã,½ãf•ãf^ã,|ã,šã,ć
- SD-WAN vEdge ã,ãfãã,|ãf%ããf«ãf¼ã,ć
- SD-WAN vEdge ãããf¼ã,ć
- SD-WAN vSmart ã,³ãf³ãf^ãfãf¼ãfãã,½ãf•ãf^ã,|ã,šã,ć

ã»žéç-

ã"ã®è,,†ã¼±æ€šã«ã³ã†|ã™ã,ã»žéç-ã-ã,ã,šã³¼ã»ã,"ã€,

ç®|ç†è€...ã-ã,ćã,ã,»ã,¹ã^¶ã¼ããfãã,¹ãf^¼^ACL¼%ãã,'ã½çç"ã—ã|ã€Cisco SD-WAN

vManage ã,½ãf•ãf^ã,|ã,šã,ćãfããfãã,»ãf¼ã,ãf³ã,°ã,ãfã¼ãf^ã,¹ãšã½çç"ãã•ã,Ĉã,ć TCP

ãfããf¼ãf^ 4222ã€6222ã€ãšã,^ã³ 8222

ã,ãf-ãfãfã,ãšãšãã³¼ã™ã€,ç°ãçfã«ãçœã~ã|ã€æ-ãã®æ-¹æ³•ãšè"ã®šãšã

- Cisco IOS ãf†ãfãã,ãã,¹ãš ACL ã,è"ã®šã—ã³¼ã™ã€,Cisco IOS ãf†ãfãã,ãã,¹ã®ã,"ã,ã,¹ãf—ãfã,ããfã,é~æçã™ã,ãæ-¹æ³•ã«ã»ã»ã,,ã|ã-ã€ããžPro [Your Core: Infrastructure Protection Access Control Listsã€ã,ã'ã,ç...šã—ã|ããããããã•ã,ã€,](#)
- Cisco SD-WAN vManage ã,½ãf•ãf^ã,|ã,šã,ćã,ãç;è-ã™ã,ããfãã,ãã,ćã,|ã,ćãf¼ãã«ãš ACL ã,è"ã®šã—ã³¼ã™ã€,Cisco éç°ãçœãžã,»ã,ãfããfããfãã,£ã,ćãf—ãfãã,ãã,ćãf³ã,¹¼^ASA¼% Cisco Firepower Threat Defense¼^FTDi¼%ã® ACL è"ã®šã«ã»ã»ã,,ã|ã-ã€ããžCisco ASA Series Firewall CLI Configuration [Guideã€ãã®ã€ĈAccess Control Listsã€ã,ã'ã,ç...šã—ã|ããããããã•ã,ã€,](#)
- Cisco ã,ãfãã,|ãf%ãã,³ãf³ãf^ãfãf¼ãfãã® ACL¼^ãã,ããf³ãfãã,|ãf³ãf%ããf«ãf¼ããf«è"±ã-ãfãã,¹ãf^¼%ãã-ã€ãã,»ãf«ãfãã,ããf¼ããf"ã,¹ãfããf ACL ã®è"ã®šãĈæ£ã—ã,,ã"ã"ã"ã,çç°èªãã™ã,ãç...è|ããĈãã,ã,šã³¼ã™ã€,ãã"ã, [WAN Cloud Hosted Controllers Provisioningã€ã,ã'ã,ç...šã—ã|ããããããããã•ã,ã€,](#)

Cisco SD-WAN vManage	First Fixed
20.6	20.6.4
20.7	20.7.1
20.8	20.8.1
20.9	20.9.1

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Cisco PSIRT

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

Product Security Incident Response Team (PSIRT);

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs>

Product Security Incident Response Team (PSIRT);

Version	Release	Fixed
1.2	20.6.4	20.6.4
1.1	20.7.1	20.7.1
1.0	20.8.1	20.8.1

å^©ç””è!ç´,,

æœ-ã,çãf%ãfã,ã,ã,ã,ãfãç,,iàçè”¼ã@ã,,ã@ããã—ã|ã”æãã¼ã—ã|ãŠã,Šã€
æœ-ã,çãf%ãfã,ã,ã,ã,ãfã@æf...å±ãŠã,ã³ãfãfã,ã@ã½ç”ã«é-çã™ã,«è²-ã»ã@ã,€
ã¼ãÿã€ã,ã,ã,ãæœ-ãf%ã,ãfãfãfãfã@ãt...ã¹ã,ã^ãŠããã—ã«ã%ãæ’ã—ã
æœ-ã,çãf%ãfã,ã,ã,ã,ãfã@è”~èç°ãt...ã¹ã«é-çã—ã|æf...å±é...ãçjã@ URL
ã,çœç•¥ã—ã€ããç<-ã@è»çè¼%ã,,,æ,,è”³ã,æ-½ã—ãÿã’ã^ã€ã½”ç¼ãÇç@çç
ã”ã@ãf%ã,ãfãfãfãfã@æf...å±ããã,ã,ã,ã,³è£½ã”ã@ã,ã³ãf%ãf!ãf¼ã,ã,ã³¼è±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。