

# Cisco Data Center Network

## Manager (DCNM) - Vulnerability in the Cisco Data Center Network Manager (DCNM) - CVE-2020-3520



Cisco Security Advisory ID : cisco-sa-

[CVE-2020-](#)

dcnm-infordisc-DOAXVvFV

[3520](#)

Published : 2020-08-19 16:00

Version : Final

CVSS Score : [5.5](#)

Workarounds : No workarounds available

Cisco Advisory ID : [CSCvt86728](#)

**Summary:** A vulnerability in the Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to execute arbitrary code on the target device.

### Details

Cisco Data Center Network

Manager (DCNM) is a software application that provides a centralized management interface for Cisco Data Center Network (DCN) devices. It is used to manage and configure DCN devices, including routers, switches, and firewalls.

The vulnerability in DCNM is located in the `doaxvfv` component. It is a remote code execution (RCE) vulnerability that can be exploited by an unauthenticated, remote attacker.

The vulnerability is caused by a buffer overflow in the `doaxvfv` component. An attacker can send a specially crafted request to the `doaxvfv` component, which will cause a buffer overflow and allow the attacker to execute arbitrary code on the target device.

The vulnerability is rated as **Medium** with a CVSS score of **5.5**. The attack complexity is **Low** and the attack vector is **Remote**.

For more information, please refer to the [Cisco Security Advisory](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-infordisc-DOAXVvFV).

### References

[Cisco Security Advisory: cisco-sa-dcnm-infordisc-DOAXVvFV](#)

Published : 2020-08-19 16:00  
Version : Final  
CVSS Score : [5.5](#)  
Workarounds : No workarounds available  
Cisco Advisory ID : [CSCvt86728](#)

Summary: A vulnerability in the Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to execute arbitrary code on the target device.

Details: The vulnerability in DCNM is located in the `doaxvfv` component. It is a remote code execution (RCE) vulnerability that can be exploited by an unauthenticated, remote attacker.

References: For more information, please refer to the [Cisco Security Advisory](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-infordisc-DOAXVvFV).

# ã>žé❖¿ç-

ã❖"ã❖®è,,†ã¼±æ€šã❖«ã³¼ã†|ã❖™ã,ã>žé❖¿ç-ã❖-ã❖,ã,šã❖¾ã❖»ã,"ã€,

# ä¿®æ£æ, ^ã❖¿ã, ½ãf•ãf^ã, |ã,šã,ç

[ã, ½ãf•ãf^ã, |ã, šã, çã❖®ã, çãffãf—ã, °ãf-ãf¼ãf%ã, 'æœœè"Žã❖™ã, <és>ã❖«ã❖-ã€ã❖,ã,ã,ã,³](#)

ã,»ã,ãf¥ãfãftã,£ã,çãf%ããf❖ã,ãã,¶ãfã

ãfšãf¼ã,ã❖šã...¥æ%ã❖šã❖❖ã,ã,ã,ã,ã,³è£½ã"❖ã❖®ã,çãf%ããf❖ã,ãã,¶ãfã,ã®šæœÿçš,ã❖«ã❖,ç

ã,½ãfãf¥ãf¼ã,ãfšãf³ã,€ã¼ã,çç°èã❖ã❖—ã❖|ã❖❖ã❖ã❖•ã❖,,ã€,

ã❖,,ã❖šã,çã❖®ãã'ã❖^ã,,ã€ã❖,çãffãf—ã,°ãf-ãf¼ãf%ã❖™ã,ãf†ãf❖ã,ãã,ã,ã❖«ã❖❖ã^†ã❖ãfjãfçã

Technical Assistance

Centeri¼^TACi¼%ã,,ã❖—ã❖❖ã❖-ã¥ç',ã❖—ã❖|ã❖,,ã,ãfjãf³ãftãfšãf³ã,ãf—ãfãf❖ã,ããfãf¼ã❖

# ä¿®æ£æ, ^ã❖¿ãfãfãf¼ã,¹

ã...-é-æ™,ç,ã❖šã❖-ã€Cisco

DCNMã,½ãfãf^ã,|ã,šã,çãfãfãf¼ã,¹1.4(1)ã¥é™ã❖«ã❖"ã❖®è,,†ã¼±æ€šã❖«ã³¼ã❖™ã,ã¿®æ£æ

æœœã,,ã®ãã...ã❖šæœææ-°ã❖®æf...ã±ã❖«ã❖ãã,,ã❖|ã❖-ã❖ã❖"ã❖®ã,çãf%ããf❖ã,ãã,¶ãfã

IDã❖®èç³°ã,»ã,ã,ãfšãf³ã,ã®,ç...šã❖—ã❖|ã❖❖ã❖ã❖•ã❖,,ã€,

# ä,æ£ã^©ç""ã°<ã¾ã❖"ã...-ã¼ç™°èj"

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ã❖-ã€æœ-ã,çãf%ããf❖ã,ãã,¶ãfãã«è"~è¼%ã❖•ã,çã❖|ã❖,,ã,è,,†ã¼±æ€šã❖

# ã†°ã...,

æœ-è,,†ã¼±æ€šã❖-ã€ã❖,ã,ã,ã,³ã†...éf"ã❖šã❖®ã,»ã,ãf¥ãfãftã,£

ãftã,ãf^ã❖«ã,^ã❖£ã❖|ç™°è|ã❖ã,çã❖¾ã❖—ã❖ÿã€,

# URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-infordisc-DOAXVvFV>

# æ"¹è",ã±¥æ'

ãfãf¼ã,ãfšãf³	èª-æ~Ž	ã,»ã,ã,ãfšãf³	ã,ãf†ãf¼ã,¿ã,¹	æ—¥ã»
1.0	ã^ã>žã...-é-ãfãfãf¼ã,¹	-	Final	2020ã¹'8æœ^

ãf◊ãf¼ã,ãfšãf³	èª-æ~Ž	ã,»ã,ã,ãfšãf³	ã,¹ãf†ãf¹¼ã,¿ã,¹	æ—Yä»~
				19 æ—Y

## å^©ç””è!ç´,,

æœ-ã,çãf%ããf◊ã,ãã,¶ãfãã◊ç,,jã¿◊è”¼ã◊@ã,,ã◊@ã◊”ã◊—ã◊|ã◊”æ◊◊ã¾ã◊—ã◊|ã◊Šã,Šã€  
æœœ-ã,Çãf%ããf◊ã,ãã,¶ãfãã◊@æf...å±ã◊Šã,^ã◊³ãfããfãã,ã◊@ã½¿ç””ã◊«é-Çã◊™ã,«è²-ã»ã◊@ã,€  
ã◊¾ã◊Yã€◊ã,ã,¹ã,³ã◊-æœœ-ãf%ãã,ãfããf;ãf³ãf^ã◊@ãt...ã@¹ã,ã°^ãŠã◊ãã◊—ã◊«ã%ãœ’ã◊—ã◊  
æœœ-ã,çãf%ããf◊ã,ãã,¶ãfãã◊@è”~è¿ãt...ã@¹ã◊«é-Çã◊—ã◊|æf...å±é...◊ã¿ã◊@ URL  
ã,çœ◊ç•Yã◊—ã€◊å◊~ç<-ã◊@è»Çè¼%ãã,,æ,,◊è”³ã,’æ-½ã◊—ã◊Yã’ã◊^ã€◊å½”ç¾¾ã◊Çç@çç◊  
ã◊”ã◊@ããf%ãã,ããfããf;ããf³ããf^ã◊@æf...å±ã◊-ã€◊ã,ã,¹ã,³è£½ã”◊ã◊@ã,ãf³ããf%ããf!ããf¼ã,¶ã,ã³¾è±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。