

# Cisco Vision Dynamic Signage

## Director



Product ID : cisco-sa-

[CVE-2020-](#)

cvdsd-rbac-y9LM5jw4

[3485](#)

Medium

Published : 2020-08-19 16:00

Version : 1.0 : Final

CVSS Score : [6.3](#)

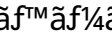
Workarounds : No workarounds available

Cisco ID : [CSCvs98756](#)

Product ID : cisco-sa-cvdsd-rbac-y9LM5jw4

Medium

Cisco Vision Dynamic Signage

Director         

The vulnerability is located in the WebContent directory of the Dynamic Signage application. It allows an attacker to access sensitive information via HTTP.

The vulnerability is a result of a missing authorization check in the WebContent directory. An attacker can exploit this to access sensitive information.

Product ID : cisco-sa-cvdsd-rbac-y9LM5jw4

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-rbac-y9LM5jw4>

Medium

Product ID : cisco-sa-cvdsd-rbac-y9LM5jw4

Published : 2020-08-19 16:00

Version : 1.0 : Final

Workarounds : No workarounds available

Product ID : cisco-sa-cvdsd-rbac-y9LM5jw4

Published : 2020-08-19 16:00

Medium



æ''è'',â±¥æ'

ãf◊ãf¼ã,ãfšãf³	è <sup>a</sup> -æ~Ž	ã,»ã,~ã,ãfšãf³	ã,¹ãf†ãf¹¼ã,¿ã,¹	æ—¥ä»~
1.0	â^◊â>žâ...-é-ãfãfãf¼ã,¹	-	Final	2020 â¹' 8 æœ^ 19 æ—¥

â^©ç''è!◊ç',,

æœ-ã,çãf%ãf◊ã,ã,ã,¶ãfã◊-ç,,jâ¿◊è''¼ã◊ã,,ã◊ã◊''ã◊-ã◊|ã◊"æ◊◊ã¾ã◊-ã◊|ã◊Šã,Šã€  
 æœ-ã,çãf%ãf◊ã,ã,ã,¶ãfã◊◊æf...â±ã◊Šã,^ã◊³ãfãfãfã,~ã◊ã¹¿ç''ã◊«é-çã◊™ã,«è²-ã»ã◊ã◊,€  
 ã◊¾ã◊Ÿã€◊ã,ã,¹ã,³ã◊-æœ-ãf%ãf,ãfãfãfãfãfã^ã◊ãt...ã¹ã,'ã^ãŠã◊ãã◊-ã◊«ã±%æ'ã◊-ã◊  
 æœ-ã,çãf%ãf◊ã,ã,ã,¶ãfã◊◊è''~è¿ãt...ã¹ã◊«é-çã◊-ã◊|æf...â±é...◊äjã◊◊ URL  
 ã,çœ◊ç•¥ã◊-ã€◊â◊ç<-ã◊◊è»çè¼%ã,,æ,,◊è''³ã,'æ-½ã◊-ã◊Ÿã'ã◊^ã€◊ã½"ç¾¾ã◊€ç◊ç◊  
 ã◊"ã◊ã◊ãf%ãf,ãfãfãfãfãfã^ã◊æf...â±ã◊-ã€◊ã,ã,¹ã,³è£½ã"◊ã◊ã, ''ãfãf%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。