

# Cisco Unified Customer Voice Portal Denial of Service (DoS) Vulnerability



Cisco-SA-20180117-cvp

[CVE-2018-0086](#)

Published: 2018-01-17 16:00

Updated: 2018-02-15 20:49

Version: 1.1 : Final

CVSS Score: 8.6

Workarounds: No workarounds available

Cisco ID: [CSCve85840](#)

Denial of Service (DoS) Vulnerability in Cisco Unified Customer Voice Portal

## Summary

Cisco Unified Customer Voice Portal (CVP) is a cloud-based contact center solution. A Denial of Service (DoS) vulnerability was discovered in CVP, which could be exploited to cause a denial of service to the affected system.

The vulnerability is located in the Cisco Virtualized Voice Browser (CVP) component. It is triggered by a SIP INVITE request containing a specific payload. The vulnerability is a Denial of Service (DoS) vulnerability, which can be exploited to cause a denial of service to the affected system.

The vulnerability is a Denial of Service (DoS) vulnerability, which can be exploited to cause a denial of service to the affected system.

For more information, please refer to the following link:  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-cvp>

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

è,,†å¼±æ€šã®ã,ã,«è½å”

ã”ã®è,,†å¼±æ€šã¬ã€11.6(1) ã,^ã,Šã%ã®ã,½ãf•ãf^ã,|ã,šã,ç  
ãfãfãf¼ã,¹ã,â®ÿè;Eã—ã|ã,,ã,« Cisco Unified CVP ã«å½±éÿã—ã¾ã™ã€,

ã®ÿè;Eã•ã,Eã|ã,,ã,« Cisco Unified CVP ã,½ãf•ãf^ã,|ã,šã,ç  
ãfãfãf¼ã,¹ã®ã^ã¥ã¬ã€ç®;ç†è€...ãE Web ãf-ãfã,|ã,¶ã,¹ã½ç”ã—ã|  
HTTPS çμEç”±ãš Cisco Unified CVP  
ã,¬ãfã,ã,çãf³ãf^ã«æŽ¥ç¶šã™ã,ãã”ã”ã«ã,^ã£ã|ã®ÿæ-½ãšã¾ã¾ã™ã€ãf

Cisco Unified Customer Voice Portal  
Version 11.5(1)

è,,†å¼±æ€šã,¹ã«ã,“ãšã,,ãªã,,ã”ã”ãçç°èªã•ã,Eãÿè½å”

ã»ã®ã,ã,¹ã,³è½å”ã«ãšã,,ã|ã€ãã”ã®ã,çãf%ããã,ã,¶ã,¶ãfã®å½±éÿã,¹ã—ã

### ã»žéç-

ã”ã®è,,†å¼±æ€šã«ã¾ã†|ã™ã,ã»žéç-ã¬ã,ã,šã¾ã»ã,“ãEã€ã”ã®è,,†å¼±æ

1)Cisco UCCE(Unified Contact Center  
Enterprise)ã,ããf³ãf•ãfã,¹ãf^ãfã,¬ãfãf£ãEã€ä;é¼ãšããã,«IPã,çãf%ããf-ã,¹ã«ã,%ã®ç

2)  
CVPã”ISPã®é-“ã«ã~ãœ”ã™ã,ã,μãf¼ãf%ããf¼ãfãfã,£ã,²ãf¼ãf^ã,|ã,šã,ããšã€ã,æ£ãª

### ä;®æ£æ,^ãçã,½ãf•ãf^ã,|ã,šã,ç

ã,ã,¹ã,³ã¬ã”ã”ã®ã,çãf%ããã,ã,¶ã,¶ãfã«è”~è¼%ãã•ã,Eãÿè,,†å¼±æ€šã«ã¾ã†|ã™ã,«ç,  
ãfãf¼ã,ãfšãf³ã”ãf•ã,£ãf¼ãfãf£

ã,»ãffãf^ã«ã¾ã—ã|ã®ãçã”ãªã,šã¾ã™ã€ããã®ã,^ã†ãªã,½ãf•ãf^ã,|ã,šã,

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html>

ã¾ãÿã€ãšã®çæš~ãEã,½ãf•ãf^ã,|ã,šã,çã,¹ãfã,|ãf³ãfãf¼ãf%ãšããã,ãã®ã¬ã€ã,



æœ%åŠ'ã,µãf¼ãf'ã,¹ã¥ç',ã,ãŠæŒã;ã®ãŠå®çæS~ã-ã€Cisco.comã®

### Software

Centerã<ã,%åãf;ã,ãfŒãf¼ãfãfãf¼ã,¹ã®à;®æfæ,^ãçã,½ãfãf^ã,|ã,Sã,çã,'ãf€ã,|ãf³ãfãf¼ãf%åã

[ãf€ã,|ãf³ãfãf¼ãf%åã>ãf¼ãf (Downloads Home)] > [è£¼ã'(Products)] >

[ã,«ã,¹ã,çãfžãf¼ã,³ãf©ãfœãf-ãf¼ã,ãfšãf³(Customer Collaboration)] >

[ã,³ãf³ã,çã,ãf^ã,»ãf³ã,çãf¼ã,½ãfããfãf¼ã,ãfšãf³ç"ã,ãf-ã,ãfšãf³(Options for Contact Center Solutions)] > [Unified Customer Voice

Portal]ã®éã«çš»ãã-ã|ããããããã,ã€,

ä,æ£ã^©ç"ã°<ã¾ã"ã...-ã¼ç™°è; "

### Cisco Product Security Incident Response

Teami¼^PSIRTi¼%åã-ã€æœ-ã,çãf%åãfã,ãã,¶ãfãã«è~è¼%åãã,Œãã|ãã,ã,è,,ã¼±æ€Sã

ã±°ã...,

ã"ã®è,,ã¼±æ€Sã- Cisco TAC

ã,µãfãf¼ãf'ã,±ãf¼ã,¹ã®èš£æ±°ã,ãç™°è|ãã,ã,Œã¾ãã-ãYã€,

### URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-cvp>

æ''è,,ã±Yæ'

ãfãf¼ã,ãfšãf³	èª-æž	ã,»ã,ã,ãfšãf³
1.1	ä;®æfæ,^ãçã,½ãfãf^ã, ã,Sã,çã®è;ã,è;½ãšã€ã,	ä;®æfæ,^ãçã,½ãfãf^ã, ã,Sã,
1.0	ã^ãžã...-é-<ãfãfãf¼ã,¹	-

ã^©ç"è|ç',,

æœ-ã,çãf%åãfã,ãã,¶ãfããç,,ãçèè¼ã®ã,,ãããããã-ãã|ã"æããã¾ãã-ãã|ãŠã,Šã€æœ-ã,çãf%åãfã,ãã,¶ãfãã®æf...ã±ãšã,^ã³ãfãf³ã,ãã®ã½çç"ãã«é-çã™ã,è²-ã»ãã®ã,ã¾ããYã€ã,ã,¹ã,³ã-æœ-ãf%åã,ãfãfãfãf³ãf^ãã®ããt...ã®¹ã,'ã°ã'Sãããã-ãã«ã%åãæ'ãã-ããæœ-ã,çãf%åãfã,ãã,¶ãfãã®èè~èç°ããt...ã®¹ã«é-çãã-ãã|æf...ã±é...ãçããã® URL

ã,çœççç¥ãã-ã€ãããç<-ãã®è»çè¼%åã,,,æ,,èè³ã,æ-½ãã-ããYã'ã^ã€ã½"ç³¾ããŒç®;çããã"ãã®ãf%åã,ãfãfãfãf³ãf^ãã®æf...ã±ãã-ããã,ã,¹ã,³è£¼ã"ãã®,ãf³ãf%åãf|ãf¼ã,¶ã,ã¾ãè±;ã

## 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。