

# Cisco TelePresence System

## MXP, a vulnerability in the Cisco TelePresence System



Product: Cisco TelePresence System  
ID: cisco-sa-20140430-mxp

Published: 2014-04-30 16:00

Version: 1.0 : Final

CVSS: 7.8

Workarounds: No Workarounds available

Cisco ID: CSCty45733 CSCty45745

CSCty45720 CSCty45731 CSCty78722

CSCty45739

[CVE-2014-2160](#)

[CVE-2014-2161](#)

[CVE-2014-2157](#)

[CVE-2014-2158](#)

[CVE-2014-2156](#)

[CVE-2014-2159](#)

Summary: A vulnerability in the Cisco TelePresence System allows an attacker to bypass authentication and gain access to the system.

### Details

Cisco TelePresence System

MXP, a vulnerability in the Cisco TelePresence System, allows an attacker to bypass authentication and gain access to the system.

- SIP @DoS, t1/4±æ€§3ä»¶
- H.225 @DoS, t1/4±æ€§3ä»¶

Impact: An attacker can bypass authentication and gain access to the system.

References: [Heartbleed](#), [OpenSSL](#), [CVE-2014-0160](#)

Heartbleed is a vulnerability in the OpenSSL library that allows an attacker to read memory from the process.

OpenSSL is a widely used cryptographic library that provides a secure communications protocol.

CVE-2014-0160 is a vulnerability in the OpenSSL library that allows an attacker to read memory from the process.

Heartbleed is a vulnerability in the OpenSSL library that allows an attacker to read memory from the process.

OpenSSL is a widely used cryptographic library that provides a secure communications protocol.

CVE-2014-0160 is a vulnerability in the OpenSSL library that allows an attacker to read memory from the process.

Heartbleed is a vulnerability in the OpenSSL library that allows an attacker to read memory from the process.

OpenSSL is a widely used cryptographic library that provides a secure communications protocol.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140430-mxp>



Security(TLS)çµCEç'±ã Šé€ ä;ã •ã,CEã Yãf;ãffã,»ãf¼ã,,ã,ã½±éYã,'ã —ã 'ã ¾ã™ã€,UDPã€

ã"ã,CEã,%ã@è,,tä¼±æ€Sã-ã€ Cisco Bug ID

CSCty45739(ç™»éCE²ãf|ãf¼ã,¶ã°,ç"")ã€ CSCty45733(ç™»éCE²ãf|ãf¼ã,¶ã°,ç"")ã€ã Šã,^ã³CSCty

Common Vulnerabilities and Exposures(CVE)IDã "ã —ã |ã€ CVE-2014-2156ã€ CVE-2014-2157ã€ã Šã,^ã³ CVE-2014-2158ã€ CEã%²ã,Šã½"ã |ã,%ã,CEã |ã,,ã¾ã™ã€,

èçæ°ã@H.225ã,µãf¼ãf"ã,¹æ'ã |ã@è,,tä¼±æ€S

Cisco TelePresence System

MXPã,ãfãf¼ã,°ã,½ãfãf^ã,lã,šã,çã@H.225ã,³ãf¼ãf%ã@èçæ°ã@è,,tä¼±æ€Sã«ã,^ã,Šã€èª€

ã"ã,CEã,%ã@è,,tä¼±æ€Sã-ã€ã Šã!™ã«ç'°ã¥ã•ã,CEã YSIPãfã,±ãffãf^ã,,ã,æ£ãªSIPã

ã"ã,CEã,%ã@è,,tä¼±æ€Sã-ã€ Cisco Bug ID

CSCtq78722i¼^ç™»éCE²ãf|ãf¼ã,¶ã°,ç"i¼%ã€ CSCty45745(ç™»éCE²ãf|ãf¼ã,¶ã°,ç"")ã€ã Šã,^ã

CVE-2014-2159ã€ CVE-2014-2160ã€ã Šã,^ã³ CVE-2014-2161ã€@CVE IDã€ CEã%²ã,Šã½"ã |ã,%ã,CEã |ã,,ã¾ã™ã€,

ãžéç-

ã"ã,CEã,%ã@è,,tä¼±æ€Sã,'è»½æ,ã™ã,ãžéç-ã-ã,ã,Šã¾ã>ã,"ã€,

ã;@æ£æ,^ãçã,½ãfãf^ã,|ã,šã,ç

ã,½ãfãf^ã,lã,šã,çã@ã,çãffãf—ã,°ãf-ãf¼ãf%ã,'æçœè"Žã™ã,ã'ã^ã-ã€ <http://www.cisco.com/g>

[ã@ã,ã,¹ã,³ã,»ã,ãfãfãftã,f](#)

[ã,çãf%ããã,ã,¶ã,¶ããã€ã;œç"ã€ã Šã,^ã³éçšYã@ã,çãf¼ã,«ã,ããf-ã,,ã€ã¾CEç¶šã@ã,çã](#)

[ã,½ãfãfãf¼ã,ãfšãf³ã,çç°èªã-ã|ããããã•ã,,ã€](#)

ã,,ã Šã,CEã@ã'ã^ã,,ã€ã,çãffãf—ã,°ãf-ãf¼ãf%ã™ã,ãfãfãã,ã,¹ã«ãããã^täªãfãfã

Technical Assistance

Centeri¼^TACi¼%ã,,ã-ãããã-ã¥ç',ã-ã|ã,,ã,ãfãf³ãftãfšãf³ã,¹ãf-ãfãfã,ããfãf¼ã€

ã"ã@ã,»ã,ãfãfãftã,£ã,çãf%ããã,ã,¶ã,¶ããã«è"i¼%ã•ã,CEã|ã,,ã,ã™ã¹ã|ã@è,,

TelePresence System



## 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。