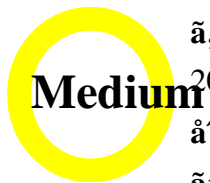


Cisco Integrated Management

Controller [®], Web Interface, API, Management Console, CLI, GUI



Product ID : Cisco-SA-

[CVE-2014-](#)

20141118-CVE-2014-7996

[7996](#)

Published : 2014-11-18 19:20

Version : 1.0 : Final

CVSS Score : [4.3](#)

Workarounds : No Workarounds available

Cisco Bug ID : [CSCuq45477](#)

CVSS Score: 4.3 (Medium)

Summary

Cisco Integrated Management

Controller (IMC) Web Interface, API, Management Console, CLI, GUI

A remote authenticated user can exploit a vulnerability in the Controller (IMC) Web Interface, API, Management Console, CLI, GUI to execute arbitrary code.

The vulnerability is caused by a buffer overflow in the Controller (IMC) Web Interface, API, Management Console, CLI, GUI.

The vulnerability is rated as Medium (CVSS Score: 4.3) because it allows a remote authenticated user to execute arbitrary code.

Workarounds: No workarounds are available for this vulnerability.

References

Additional information is available in the following references:

Bug ID [CSCuq45477](#), [Cisco](#)

Impact

The vulnerability allows a remote authenticated user to execute arbitrary code on the Controller (IMC) Web Interface, API, Management Console, CLI, GUI.

ãf ¼ã,ãfšã³	èª~æŽ	ã,»ã,ã,ãfšã³	ã,¹ãf†ãf¼ã,¼ã,¹	æ—Ÿä»~
1.0	â^ç%ãfãfãf¼ã,¹	é©ç””â±-	Final	2014â¹¹1æce¹8æ—Ÿ

â^ç””è!ç´,,

æce-ã,çãf%ãfã,ã,ã,ãfããç,,jãçè”¼ã@ã,,ã@ããã—ã|ã”æãã¼ãã—ã|ãŠã,Šã€
æce-ã,çãf%ãfã,ã,ã,ãfãã@æf...â±ãŠã,ãããfããã,ãã@ã¼çç””ã«é-çã™ã,«è²-ã»ã@ã,€
ã¼ããŸã€ã,ã,¹ã,³ã-æce-ãf%ãã,ãfãfãfãããã@ãt...ã@¹ã,ã^ãŠããã—ã«ã%ãæ’ã—ã€
æce-ã,çãf%ãfã,ã,ã,ãfãã@è”~èç°ãt...ã@¹ã«é-çã—ã|æf...â±é...ãçjã@ URL
ã,çceçç•ã—ã€ããççãã@è»çè¼%ã,,,æ,,è”³ã,æ-½ã—ãŸã’ã^ã€ã¼”çã¼ãã€ççççç
ã”ã@ãf%ãã,ãfãfãfãããã@æf...â±ã-ã€ã,ã,¹ã,³è£½ã”ã@ã,ãfãf%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。