

# Cisco SocialMiner

## XML External Entity (XXE) Processing



Cisco-SA-20170906-socmin

[CVE-2017-12216](#)

20170906-socmin

Published: 2017-09-06 16:00

Version: 1.0 : Final

CVSS Score: 6.5

Workarounds: No workarounds available

Cisco ID: [CSCvf47946](#)

Summary: An XML External Entity (XXE) processing vulnerability in Cisco SocialMiner allows an attacker to read arbitrary files on the server.

### Details

Cisco

SocialMiner is a web application that uses XML External Entity (XXE) processing to parse XML data.

The vulnerability is located in the XML parser component of SocialMiner.

When an XML document is processed, the parser incorrectly handles external entities, allowing an attacker to inject arbitrary content.

XXE vulnerability details and mitigation information.

[https://www.owasp.org/index.php/XML\\_External\\_Entity\\_\(XXE\)\\_Processing](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)

Additional information regarding the vulnerability and its impact.

For more details, please refer to the Cisco Security Advisory: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-socmin>

### Conclusion

This vulnerability is a Medium severity issue that affects Cisco SocialMiner.

It is recommended that users update to the latest version of SocialMiner.

For more information, please refer to the Cisco Security Advisory: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-socmin>

Bug ID: CSCvf47946

è,†å¼±æ€šã,â«ã,“ãšã,,ãªã,,ã“ã “ã Çç°èªã•ã,Œãÿè½å”  
ä»-ã®ã,ã,¹ã,³è½å”ã«ãšã,,ã|ã€ã“ã®ã,çãf%ãfã,ã,¶ã,¶ãfã®ã½±éÿã,â—ã

### åž�éç-

ã“ã®è,†å¼±æ€šã«ã¼å†|ã™ã,ãžéç-ã-ã,ã,šã¾ãã,“ã€,

### äç®æ£æ,^ãçã,½ãf•ãf^ã,|ã,šã,ç

äç®æ£æ,^ãçã,½ãf•ãf^ã,|ã,šã,ç  
ãfªãfªãf¼ã,¹ã®èç°ã«ãªã,,ã|ã-ã€æœ-ã,çãf%ãfã,ã,¶ã,¶ãfã,šéf”ã® Cisco  
Bug ID ã,âç...šãçãããã•ã,,ã€,

ã,½ãf•ãf^ã,|ã,šã,çã®ã,çãffãf—ã,°ãf-ãf¼ãf%ã,æœœè”žã™ã,éšã«ã-ã€[ã,ã,¹ã,³ã®ã,»ã,ãf  
Security Advisories and Alerts¼%]  
ãfšãf¼ã,ãšã...¥æ%ãšãçãã,ã,ã,¹ã,³è½å”ã®ã,çãf%ãfã,ã,¶ã,¶ãfã,â®šæœÿçš,,ã«ãç,ç  
ã,½ãfªãf¼ã,ãfšãf³ã,çç°èªã—ã|ãçãããã•ã,,ã€,

ã,,ãšã,Œã®ã á^ã,,ã€ã,çãffãf—ã,°ãf-ãf¼ãf%ã™ã,ãfªãfã,ã,¹ã«ãã^ãªãfãfçã  
Technical Assistance  
Center¼^TAC¼%ã,,ã—ãçã-ã¥ç’,,ã—ã|ã,,ã,ãfãf³ãfãfšãf³ã,¹ãf—ãfãfã,ããfãf¼ã«

### ä,æ£ã^ç””ã°ã¾ã”ã...-ã¼ç™°èj”

Cisco Product Security Incident Response  
Team¼^PSIRT¼%ã-ã€æœ-ã,çãf%ãfã,ã,¶ã,¶ãfã«è”~è¼%ã•ã,Œã|ã,,ã,è,†å¼±æ€šã

### å†°å...,

ã,ã,¹ã,³ã-ã€ãã“ã®è,†å¼±æ€šã,ç™°è|ã—ã€ã±ãšã—ã|ã,,ãÿããã,ãÿã,»ã,ãf  
Gocylæ°ã«æ,,ÿè-ã,,ãÿã—ã¾ã™ã€,

### URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-socmin>

### æ”¹è,å±¥æ’

ãfãf¼ã,ãfšãf³	èª~ž	ã,»ã,ã,ãfšãf³	ã,¹ãfªãf¼ã,çã,¹	æ—¥ã»~
1.0	ã^ãžã...-é-ãfªãf¼ã,¹	-	Final	2017 å¹´ 9 æœˆ 6 æ—¥

å^©ç””è!ç´,,

æœ-ã,çãf%ãfã,ã,ã,ã,ãfãç,,iàçè”¼ã@ã,,ã@ã”ã—ã|ã”æãã¼ã—ã|ãŠã,Šã€  
æœ-ã,çãf%ãfã,ã,ã,ã,ãfã@æf...å±ãŠã,^ã³ãfãfã,ã@ã½ç””ã«é-çã™ã,«è²-ä»ã@ä,€  
ã¼ãÿã€ã,ã,ã,ãæœ-ãf%ã,ãfãfãfãfã@ãt...ã¹ã,ã^ãŠãã—ã«ã%ãæ’ã—ã  
æœ-ã,çãf%ãfã,ã,ã,ã,ãfã@è”~èç°ãt...ã¹ã«é-çã—ã|æf...å±é...ãçjã@ URL  
ã,çœç•¥ã—ã€ããç<-ã@è»çè¼%ã,,,æ,,è”³ã,æ-½ã—ãÿã’ã^ã€ã½”ç¼ãÇç@çç  
ã”ã@ãf%ã,ãfãfãfãfã@æf...å±ãæã,ã,ã,ã,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。