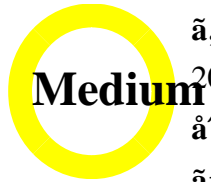


Cisco ASR 5500 System Architecture Evolution Gateway GPRS Tunneling Protocol (GTP) DoS, Denial of Service



Cisco-SA-20170906-asr

[CVE-2017-12217](#)

Published: 2017-09-06 16:00

Version: 1.0 : Final

CVSS Score: 5.8

Workarounds: No workarounds available

Cisco Bug ID: [CSCve07119](#)

Denial of Service (DoS) vulnerability in Cisco ASR 5500 System Architecture Evolution (SAE) Gateway GPRS Tunneling Protocol (GTP)...

Impact

Cisco ASR 5500 System Architecture Evolution (SAE) Gateway GPRS Tunneling Protocol (GTP) Denial of Service (DoS) vulnerability...

The vulnerability is located in the GTP Tunneling Protocol (GTP) component of the SAE software. It is a Denial of Service (DoS) vulnerability that can be exploited by sending specially crafted packets to the affected device.

Affected Versions: Cisco ASR 5500 SAE 1.0

Workarounds: No workarounds are available at this time.

CVSS Score: 5.8 (Medium)

For more information, please refer to the following URL:

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

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Medium severity rating

ASR 5500 System Architecture Evolution (SAE) Gateway GPRS Tunneling Protocol (GTP) Denial of Service (DoS) vulnerability...

Evolution (SAE) Gateway GPRS Tunneling Protocol (GTP) Denial of Service (DoS) vulnerability... Bug ID: CSCve07119

è,,†á¼±æ€šã,'ã«ã,"ãšã,,ãªã,,ã"ã "ã Ççç°èªã•ã,Œãÿè½á"

ã»-ã®ã,ã,¹ã,³è½á"ã«ãšã,,ã|ã€ã"ã®ã,çãf%ããã,ãã,¶ãfãã®ã½±éÿã,á-ã

ãžéç-

ã"ã®è,,†á¼±æ€šã«ã¾á†|ã™ã,ãžéç-ã-ã,ã,šã¾ãã,"ã€,

ã;®æ£æ,^ãçã,½ãf•ãf^ã,|ã,šã,ç

ã;®æ£æ,^ãçã,½ãf•ãf^ã,|ã,šã,ç

ãfªãfªãf¼ã,¹ã®èç³ç°ã«ããã,,ã|ã-ã€æœ-ã,çãf%ããã,ãã,¶ãfãã,šéf"ã® Cisco Bug ID ã,á,ç...šãããããã•ã,,ã€,

ã,½ãf•ãf^ã,ã,šã,çã®ã,çãffãf-ã,°ãf-ãf¼ãf%ãã,'æœœè"žã™ã,éšã«ã-ã€[ã,ã,¹ã,³ã®ã,»ã,ãf Security Advisories and Alerts¼%]

ãfšãf¼ã,,ãšã...¥æ%ããšãããã,ã,ã,¹ã,³è½á"ã®ã,çãf%ããã,ãã,¶ãfãã,á®šæœÿçš,,ã«ã,çãã,½ãfªãf¼ã,ãfšãf³ã,çç°èªã-ã|ãããããã•ã,,ã€,

ã,,ãšã,Œã®ã á^ã,,ã€ã,çãffãf-ã,°ãf-ãf¼ãf%ãã™ã,ãfªããã,ãã,¹ã«ããã^ãªãfãfçãã Technical Assistance

Center¼^TAC¼%ã,,ã-ãããã-ã¥ç',ã-ã|ã,,ã,ãfãf³ãfãfšãf³ã,¹ãf-ãfããã,ããfãf¼ãã«

ã,æ£ã^ç"ã°ã¾ãã"ã...-ã¼ç™°èj"

Cisco Product Security Incident Response

Team¼^PSIRT¼%ã-ã€æœ-ã,çãf%ããã,ãã,¶ãfãã«è"~è¼%ãã•ã,Œã|ã,,ã,è,,†á¼±æ€šã

ã†°ã...,

ã"ã®è,,†á¼±æ€šã Cisco TAC

ã,¶ãfãf¼ãf^ã,±ãf¼ã,¹ã®èš£æ±°ã,ã«ç™°è|ããã,Œã¾ãã-ãÿã€,

URL

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

æ"¹è",ã±¥æ'

ãfãf¼ã,ãfšãf³	èªæž	ã,»ã,ã,ãfšãf³	ã,¹ãfªãf¼ã,çã,¹	æ-¥ã»
1.0	ã^ãžã...-é-ãfªãfªãf¼ã,¹	-	Final	2017 á¹ 9 æœ^ 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。