

Cisco

Guardã«ã,^ã,<ã,¬ãfã,¹ã,µã,¤ãf^ã,¹ã,¬ãf¹ãf—ãf



ã,¢ãf‰oãf♦ã,¤ã,¶ãf¹ãf¹ID : cisco-sa-
20060920-guardxss

[CVE-2006-4909](#)

å^♦å...¬é-æ—¥ : 2006-09-20 16:00

æœ€qæ>`æ—°æ—¥ : 2012-01-02 12:18

ãf♦ãf¹ã,ãf§ãf³ 1.1 : Final

CVSSã,¹ã,³ã,¢ : [1.9](#)

å›žé♦¿ç- : No Workarounds available

Cisco ãf♦ã,° ID :

æ—¥æœ¬è^zã♦«ã,^ã,<æf...å ±ã♦¬ã€♦è<±è^zã♦«ã,^ã,<åŽÝæ-‡ã♦®é♦žå...¬å¹¼♦ã

æ!,è!♦

Cisco

Guardã♦®è,,†å¹¼±æ€§ã♦«ã,^ã,Šã€♦Guardã♦ŒWebãf-ãf©ã,|ã,¶ã,¬ãf©ã,¤ã,¢ãf³ãf^ã♦“Webã,µãf¹

ã♦“ã♦®ã,¢ãf‰oãf♦ã,¤ã,¶ãf¹ãf^ã♦¬ã€♦<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory-20060920-guardxss>ã♦§å...¥æ‰oã♦§ã♦§ã♦§¾ã♦™ã€,

è©²å¹/2“è£¹/2å“♦

ã♦“ã♦®ã,»ã,¬ã,·ãf§ãf³ã♦«ã♦¬ã€♦è©²å¹/2“è£¹/2å“♦ã♦«é-çã♦™ã,«è©³ç’ºã♦ŒæŽ²è¹¼‰ã♦•ã,Œã♦

è,,†å¹¼±æ€§ã♦®ã♦,ã,<è£¹/2å“♦

æ¬|ã♦®ã,·ã,¹ã,³è£¹/2å“♦ã♦«ã♦¬è,,†å¹¼±æ€§ã♦Œå~åœ”ã♦—ã♦§¾ã♦™ã€,

- Cisco Guardã,¢ãf—ãf©ã,¤ã,¢ãf³ã,¹(1/4^ã,1/2ãf•ãf^ã,|ã,§ã,¢ãf♦ãf¹ã,ãf§ãf³3.X¹¼‰)
- Cisco Guard Bladei¹/4^ã,1/2ãf•ãf^ã,|ã,§ã,¢ãf♦ãf¹ã,ãf§ãf³4.X¹¼‰)
- Cisco Guardã,¢ãf—ãf©ã,¤ã,¢ãf³ã,¹(ã,1/2ãf•ãf^ã,|ã,§ã,¢ãf♦ãf¹ã,ãf§ãf³5.0(3))
- Cisco Guardã,¢ãf—ãf©ã,¤ã,¢ãf³ã,¹(ã,1/2ãf•ãf^ã,|ã,§ã,¢ãf♦ãf¹ã,ãf§ãf³5.1(5))

è,,†å¹¼±æ€§ã,’å♦«ã,“ã♦§ã♦„ã♦³ã♦„ã♦“ã♦”ã♦”ã♦Œççºè^ã♦ã♦•ã,Œã♦Ÿè£¹/2å“♦

ã»—ã♦®ã,·ã,¹ã,³è£¹/2å“♦ã♦«è,,†å¹¼±æ€§ã♦¬è|ã♦¤ã♦ã♦£ã♦|ã♦„ã♦§¾ã♦>,“ã€,

Cisco Guard

DDoSè½æ, »å¬¾ç—ã, çäf—ãf©ã, ãä, çäf³ã, ¹ã♦§å®Ýè;Œã♦•ã,Œã♦|ã♦,,ã,½äf•äf^ã, |ã,§ã,çäf♦äf¼ã,

- ä»®æf³ç«-æœ«ã♦¾ã♦Ýã♦-äfäf¼ã, «äf«ã, ·äf^ã, çäf«ã, ³äf³ã, ½äf¼äf«æŽ¥ç¶š
äfäf¼ã, «ãf«ãf»ã, ·äf^ã, çäf«ãf»ã, ³äf³ã, ½äf¼äf«ã, %oã, ½äf•äf^ã, |ã,§ã,çäf♦®äf♦äf¼ã, äf§äf³ç

Cisco Guard Version 3.1(0.12)

GUARD login:

ã♦“ã♦®ä¾<ã♦§ã♦-ã€♦Cisco

Guardä♦-ã,½äf•äf^ã, |ã,§ã,çäf♦äf¼ã, äf§äf³3.1ã, 'å®Ýè;Œã♦—ã♦|ã♦,,ã♦¾ã♦™ã€,

å»®æf³ç«-æœ«ã♦®å`å♦^ã€♦æ%oé tã♦-å♦Œã♦~ã♦§ã♦™ã♦Œã€♦ã, ·äf^ã, çäf«äf»ã, ±äf¼

- äf^äfçäf¼äf^ã, »ã,äf¥ã,çä,·ã,§äf«(SSH)æŽ¥ç¶š

SSHä, »äffä, äf§äf³ã, 'ä»<ã♦—ã♦|ã,½äf•äf^ã, |ã,§ã,çäf♦äf¼ã, äf§äf³ç•^ä♦·ã, 'å♦-å¾—ã♦™ã,

Guardä♦«ãf, °ã, ãäf³ã♦—ã€♦show

versionã, ³äfžäf³ãf%oãf©ã, ãäf³ã, ãäf¼äf•ã, §ã, ãä, ¹(CLI)ã, ³äfžäf³ãf%oã, 'ç™oè;Œã♦—ã♦¾ã♦™

<#root>

```
prompt$ ssh admin@guard.example.com
admin@guard.example.com's password:
Last login: Wed Nov 24 22:45:53 on ttys0
admin@GUARD#
```

show version

Copyright (c) 2000-2004 Cisco Systems, Inc. All rights reserved.

Software License Agreement

[...]

Cisco Anomaly Guard

Release: 3.1(0.12)

Date: 2004/10/27 19:58:14

GUARD uptime is 3 weeks, 3 days, 17 hours, 53 minutes
System Serial Number: XXXXXXXX

ã♦“ã♦®ä¾<ã♦§ã♦-ã€♦Cisco Traffic Anomaly

Guardä♦-ã,½äf•äf^ã, |ã,§ã,çäf♦äf¼ã, äf§äf³3.1ã, 'å®Ýè;Œã♦—ã♦|ã♦,,ã♦¾ã♦™ã€,

- äf^äfçäf¼äf^ã, »ã,äf¥ã,çWebä, »äffä, äf§äf³
Cisco

Guardä♦Œã, »ã,äf¥ã,çä♦^aWebä, ãäf³ã, ãäf¼äf•ã, §ã, ãä, ¹ã, 'ä»<ã♦—ã♦|å®Ýè;Œã♦—ã♦|ã♦,,ã

<https://IP>, çäf%oãf-ã, '/ã, 'é—ã♦, ã€♦äf^ã, °ã, ãäf³ã♦—ã♦|ã€♦äf-äf©ã, |ã, ¶ã, |ã, £ãf³ãf%oã, |ã

ãäf^äf³ã, -ã, 'ã, -ãäf^äffä, -ã♦—ã♦¾ã♦™ã€,

è©³çº

- ã, ¯ãf@ã,¤ã,¢ãf³ãf^ãf|ãf¹/4ã,¶ã ¯ã€♦Guardã♦«ã,^ã♦£ã♦|ã¿♦è·ã♦•ã,Œã♦|ã♦,,ã,<ã,µã,¤ãf^ã♦
 - ã,¬ãf¹/4ãf%oã ¯ã,¢ã,¬ãftã,£ãf-ã♦^ãYºæœ¬ã¿♦è·ã,'å®Ýè;Œã♦—ã€♦åYºæœ¬/ãf^ãf€ã,¤ãf¬ã,¬ã.
 - ç‰¹å~¥ã♦«å~§ã |™ã «ç~å~¥ã♦•ã,Œã?Ýhttpè;♦æ±,ã?¬ãf¹/4ãf%oã,¬ãf¹/4ãf%oã,¬ã?—ã?|è)Çé€♦

refreshã, —ä¿jä—ä€äÿä, äè¾¼ä¿ä, —äf^aäf—äf^ä, —ä‡|ç†ä—ä¾ä™ä€,

“”Bug ID

CSCsf01438(ç™»éŒœäº†äº¹ä¼,¶äº°,ç”º)äºäºç½è·¡äº•äº,Œäº|äº„äº³äº™äº,

å>žé◆?¿ç-

HTTP-
TCP-

1. $\frac{3}{4}f^{\frac{1}{4}}f^3$, 'èj^o— $\frac{3}{4}$ TM

<#root>

user@GUARD#

show zone test

... skipped

***** USER FILTERS *****

```

Row Source IP Source Mask      Proto DPort Frg Action Rate Burst Units RxRate(pps)
10 *          255.255.255.255 6       80     no   basic/redirect

user@GUARD#
config t
user@GUARD-conf#
zone test
user@GUARD-conf-zone-test#
no user-filter 10

```

2. åÑºæœ¬/ã,»äf¼äf•äfªã,»äffäf^ä♦®äf€ã,¤äfŠäfÝäffä,—äf•ä,£äf«ã,¿ã,'è „å®šä♦—ä♦¾ä♦™ã€,

```

<#root>
user@GUARD-conf-zone-test#
user-filter 10 basic/safe-reset * 6 80

```

3. äf•ä,£äf«ã,¿ã♦Œé♦©ç"“ä♦•ä,Œä♦|ä♦„ã,«ä♦"ä♦ „ã,’ç¤ºä♦—ä♦¾ä♦™ã€,

```

<#root>
user@GUARD#
show zone test
...skipped
**** USER FILTERS ****
Row Source IP Source Mask      Proto DPort Frg Action Rate Burst Units RxRate(pps)
10 *          255.255.255.255 6       80     no   basic/safe-reset

```

è©³çºä♦«ã♦¤ä♦„ã♦|ä♦—ä♦æ¬jä♦®è „å®šä,¬ã,¤äf%oã,'å♦,ç...§ä♦—ä♦|ä♦¤ä♦ ä♦•ä♦„ã€,

http://www.cisco.com/en/US/products/ps5888/products_configuration_guide_chapter09186a00804b7d13.html#wp1

ä¿®æ£æ,^ä♦¿ã,½äf•äf^ä,|ã,§ä,¢

ä♦"ä♦®è,†å¼±æ€§ä♦—ä€♦Cisco Anomaly

Guard,³äf¼äf%oã♦®äf♦äf¼ä,äf§äf³5.1(6)ä♦§ä¿®æ£ä♦•ä,Œä♦|ä♦„ã♦¾ä♦™ã€,

ä,¤äffäf—ä,ºäf¬äf¼äf%oã,’¤¤æè·Žä♦™ä,¤ä 'å♦^ä♦—ä€♦<http://www.cisco.com/go/psirt>

ã♦ .. å¾Œç¶šã♦®ã, çãf‰oãf♦ã, ãã, ¶ãfªã, , å♦, ç...§ã—ã♦ | ã€♦å•♦éjŒã♦®èñfæ±°çŠ¶æ³♦ã♦ .. å®ã, ½ãfªãf¥ãf%4ã, ·ãf§ãf³ã, 'ç¢°è^ã♦—ã♦ | ã♦?ã?ã?ã?•ã?„ã?, ã€,

ã♦ „ã?šã,Œã♦®å`å?^ã, ã€♦ã, çãffãf—ã, °ãf—ãf%4ãf‰oã♦™ã, <æ©Ýå™.. ã♦«å?♦å`å`†ã♦`ãfjãfçãfã`
Technical Assistance

Centerï¼^TACï¼‰oã♦¾ã♦Ýã?—å¥'ç „ã, 'çµã, "ã?§ã„ã, <ãfjãf³ãftãf§ãf³ã, 1
ãf—ãfãf♦ã, ãf£ãf%4ã«ã?Šå•ã?„ã?^ã?»ã?♦ã?ã? ã?•ã?„ã?, ã€,

ã?æfå`®ç”“ã°<ã¾<ã?“å...-å¼?ç™oèi”

Cisco PSIRT

ã?§ã?—ã€♦æœ-ã, çãf‰oãf♦ã, ãã, ¶ãfªã «è .. è¼‰oã?•ã,Œã?|ã?„ã, <è,,†å¼±æ€§ã?®ã, ã?æfå`®ç”“
ã?“ã?®è,,†å¼±æ€§ã?—ã€♦ã?Šå®çæ§~ã?•ã, %oã, ·ã, 1ã, ³ã «å ±å'Sã?•ã,Œã?Ýã, ã?®ã?§ã?™ã€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060920-guardxss>

æ”¹è”, å±¥æ`

ãfªãf“ã, ,ãf§ãf³ 1.1	2011å¹`1æœ^2æ—¥	è,,†å¼±æ€§ã, 1ã, ³ã, çè©³ç`°ã?®ãftãf³ãf—ãf—ãf%4ãf^ãftã, ã, 1ãf^ã, 'æ»
ãfªãf“ã, ,ãf§ãf³ 1.0	2006å¹`9æœ^20æ—¥	å^ã?å`žå...-é-<ãfªãf%4ã, 1

å`®ç”“è!♦ç“

æœ-ã, çãf‰oãf♦ã, ãã, ¶ãfªã?—ç„jä?è .. ¼ã?®ã, ã?®ã?“ã?—ã?|ã?“æ?♦æ¾?ã?—ã?|ã?Šã, Šã€
æœ-ã, çãf‰oãf♦ã, ãã, ¶ãfªã?®æf...å ±ã?Šã, ^ã?³ãfªãf³ã, —ã?®ä½?ç”“ã?«é-çã?™ã, <è²-ä»»ã?®ã, €
ã?¾ã?Ýã€♦ã, ·ã, 1ã, ³ã?—æœ-ãf‰oã, ãf¥ãfjãf³ãf^ã?®å†...å®¹ã, 'æ^å'Sã?•ã?—ã?«å¤‰æ»'ã?—ã?
æœ-ã, çãf‰oãf♦ã, ãã, ¶ãfªã?®è .. è?°å†...å®¹ã?«é-çã?—ã?|æf...å ±é...♦ä?jã?® URL
ã, 'çœ?ç?•¥ã?—ã€♦å?~ç<-ã?®è»çè¼‰oã,,æ,,?è .. ?æ-½ã?—ã?Ýã`å?^ã€♦å½“ç¤¾ã?Œç®jç?
ã?“ã?®ãf‰oã, ãf¥ãfjãf³ãf^ã?®æf...å ±ã?—ã€♦ã, ·ã, 1ã, ³èF½å“♦ã?®ã, “ãf³ãf‰oãf!ãf%4ã, ¶ã, 'å?—¾è±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。