

Cisco Clean

Accessã«ãŠã'ã,«DoSã,ã®å³¼å¿œ



ã,¢ãf%ãfã,¤ã,¶ãfªãf¼ID : cisco-sa-

20051221-CCA

å^ã...-é-«æ—¥ : 2005-12-21 22:00

ãfãf¼ã,ãfšãf³ 1.1 : Final

å»žé¿ç- : No Workarounds available

Cisco ãfã,° ID :

æ—¥æœ-èªžã«ã,^ã,«æf...å ±ã-ã€è«èªžã«ã,^ã,«åŽŸæ-#ã®éžã...-å¼ã

æ',è'¿

ã"ã,Œã-ã€Alex LansteinãŒãfjãffã,»ãf¼ã,ã€ŒDoS in Cisco Clean

Accessã€i¼^2005å¹12æœ^16æ—¥ã«Bugtraqãfjãf¼ãfªãf³ã,°ãfªã,¹ãf^ã«æŠ•ç`¿i¼%ã®ä,ãš

PSIRTã®å»žç"ãšã™ã€,ãf-ãfãf¼ãf^ã®ã,¢ãf¼ã,«ã,¤ãf-ç%ã-æ¬jã®å'æ%ã€ã«ã,ãš

<http://www.securityfocus.com/archive/1/419645/30/0/threaded>

Cisco

ãšã-ã€ç"ç©¶è€...ã"ã"ãšã-ã|ã,»ã,ãfªãfªãfªã,£è,,tå¼±æ€šã«é-¢ã™ã,«è¿æŸ»ã,é

è¿½åŠ æf...å ±

ã"ã®å•éjŒã-ã€Cisco Bug ID

CSCsc85405(ç™»éŒ²ãfjãf¼ã,¶ã°,ç")Â€Â"æ—šå¼ã®JSPãŒŒCAMã«DoSæ"»æ'fã,å¼•ã€èµ•ã

ã"ã®DDTSã-ã™ãšã«èš£æ±°ã•ã,Œã|ãšã,šã€ä¿œ£ã-ã^©ç"ã-èf½ãšã™

Cisco Clean Access

Manager(CAM)ã,'ã,¶f¼ãf"ã,¹æ'ã|(DoS)æ"»æ'fã«å³¼ã—ã|ã,ªãf¼ãf—ãf³ã®ã³¼ã³¼ã«ã

ãf'ãffãfã-ã€æ¬jã®å'æ%ã€ã,%,ãf£ã,|ãf³ãfãf¼ãf%ãšãã³¼ã™ã€,

<http://www.cisco.com/pcgi-bin/tablebuild.pl/cca-patches?psrtdcat20e2>

æ¬jã®æf...å ±ã-ã€CSCsc85405ã®ãfãffãfã«ã»~å±žã™ã,«READMEãf•ã,jã,¤ãf«ã«è"~è¹

To address and fix this vulnerability, you must remove the obsolete JSP files from your CAM as they are no longer needed. You can either:

1. Install the patch on your CAM, as described in "Patch Installation Instructions" below, or
2. Apply the workaround, as described in "Workaround Solution" below.

Caveat CSCsc85405 will be resolved in the following future releases:

- * Cisco Clean Access release 3.5(9) and above
- * Cisco Clean Access release 3.6.0.1 and above

=====
Patch Installation Instructions
=====

To install this patch:

1. Download the Patch-CSCsc85405.tar.gz file from the Cisco Clean Access Patches folder
(<http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches>) under Cisco Secure Software
(<http://www.cisco.com/public/sw-center/ciscosecure/cleanaccess.shtml>).
2. Open an SSH terminal and copy the patch file into your Clean Access Manager (CAM) using WinSCP, SSH File Transfer or PSCP, as described below.

If using WinSCP or SSH File Transfer:

- a. Copy Patch-CSCsc85405.tar.gz to the /store directory on the Clean Access Manager.

If using PSCP:

- a. Open a command prompt on your Windows computer.
- b. Cd to the path where your PSCP resides
(e.g, C:\Documents and Settings\desktop).
- c. Enter the following command to copy the file to the CAM:

```
pscp Patch-CSCsc85405.tar.gz root@ipaddress_manager:/store
```

3. From the SSH terminal, untar the patch file on the CAM:

```
cd /store  
tar xzvf Patch-CSCsc85405.tar.gz
```

4. Cd to the Patch-CSCsc85405 directory:

```
cd Patch-CSCsc85405
```

5. Execute the patch file upgrade on the CAM:

```
./patch.sh
```

=====
Workaround Solution
=====

1. Open an SSH terminal, and login to the CAM shell.
2. Change directory as follows:

3. Remove the uploadclient.jsp and ieee8021x.jsp files:

4. Change directory as follows:

5. Remove the cached jsp sources:

6. Remove any file in the "installer/window" directory, this will be useful for any exploited machine.

æœ-ã, ¢ǻf%ǻfǻ, mǻ, ¶ǻfǻ - ¸,, ä¿ è "¼ǻ ®ǻ, ã®ǻ "ǻ —ǻ |ǻ "æ¿¿ä¾ǻ —ǻ |ǻ Šǻ, Šǻ
æœ-ã, ¢ǻf%ǻfǻ, mǻ, ¶ǻfǻ ®æf...ǻ ±ǻ Šǻ, ^ǻ³ǻfǻfǻ, ~ǻ®½¿¸""ǻ «é- ¢ǻ™ǻ, <è²-ǻ»»ǻ ®ǻ, €
ǻ¿¾ǻ Ÿǻ€ǻ, .ǻ, ¹ǻ, ³ǻ - æœ-ǻf%ǻ, ǻf¥ǻfǻfǻ³ǻfǻ®ǻt...ǻ®¹ǻ, 'ǻ^ǻ'Šǻ ǻǻ —ǻ «ǻº%ǻæ'ǻ —ǻ

æœ¬ã,¢ãf%ãf❖ã,¤ã,¶ãfªã❖®è¨~è¿°å†...å®¹ã❖«é-çã❖—ã❖|æf...å±é...❖ä¿ã❖® URL
ã,'çœ❖ç•¥ã❖—ã€❖å❖~ç‹¬ã❖®è»çè¼%ã,,,æ,,❖è¨³ã,'æ-½ã❖—ã❖ÿå´å❖^ã€❖å½"ç¤¾ã❖Œç®;ç❖
ã❖"ã❖®ãf%ã,ãf¥ãf;ãf³ãf^ã❖®æf...å±ã❖¬ã€❖ã,·ã,¹ã,³è£½å"❖ã❖®ã,¨ãf³ãf%ãf!ãf¼ã,¶ã,'å³¼è±;ã

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。