

# Cisco Security Monitoring, Analysis and Response System(CS-MARS) 安全性分析報告書



严重性 ID : cisco-sa-20060719-mars

[CVE-2006-3734](#)

发布日期 : 2006-07-19 16:00

[CVE-2006-3732](#)

状态 : Final

工作绕道 : No Workarounds available

Cisco 安全性 ID :

此报告书详细描述了 Cisco 安全性分析结果，包括漏洞的性质、影响范围、修复建议等。

## 漏洞概述

Cisco Security Monitoring, Analysis and Response System(CS-MARS)

该漏洞是由于 Oracle Java 容器存在一个缓冲区溢出漏洞，导致远程攻击者可以通过发送精心构造的数据包来执行任意代码。受影响的系统包括所有运行 CS-MARS 的 Cisco 设备。

### 受影响系统

MARS 安装在运行 Oracle Java 容器的 Cisco 设备上，如 Cisco ASA、Cisco PIX、Cisco ASA 5500 等。

### 缓解措施

建议安装最新的 Cisco 安全性更新，或者禁用 Java 容器以防止该漏洞被利用。

### 漏洞利用

攻击者可以通过发送恶意构造的数据包来触发缓冲区溢出，从而执行任意代码。受影响的系统包括所有运行 CS-MARS 的 Cisco 设备。

受影响的系统包括所有运行 CS-MARS 的 Cisco 设备，如 Cisco ASA、Cisco PIX、Cisco ASA 5500 等。

建议安装最新的 Cisco 安全性更新，或者禁用 Java 容器以防止该漏洞被利用。

Cisco

有关此漏洞的更多信息，请参阅 [Cisco 安全性公告](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060719-mars)。

有关此漏洞的更多信息，请参阅 [Cisco 安全性公告](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060719-mars)。

## 结束语

感谢您使用 Cisco 安全性分析报告书。如有任何问题或疑虑，请随时与我们联系。

## è,,†å¼±æ€§ã®ã♦,ã,«è£½å“♦

4.2.1ã,^ã,Šå‰♦ã♦®ãƒ♦ãƒ¼ã,ãf§ãƒã♦®CS-

MARSã,½ãf•ãf^ã,|ã,§ã,çã♦—ã€♦ã♦“ã♦®ã,çãf‰ãf♦ã,¤ã,¶ãfã♦§èª—æ~žã♦•ã,Œã♦|ã♦,,ã,«è,,†

CS-

MARSã,½ãf•ãf^ã,|ã,§ã,çã♦®ãƒ♦ãƒ¼ã,ãf§ãƒã,’ççºèª♦ã♦™ã,«ã♦—ã€♦SSHã,—ãf©ã,¤ã,çãf³ãf^ã

```
prompt$ ssh pnadmin@10.0.0.1
pnadmin@10.0.0.1's password:
Last login: Tue Jun 20 16:22:34 2006 from 10.0.0.2
```

```
CS MARS - Mitigation and Response System
```

```
? for list of commands
```

```
[pnadmin]$ version
4.1.5 (2198)
```

## è,,†å¼±æ€§ã,’å♦«ã,“ã♦§ã♦,,ã♦³ã♦,,ã♦“ã♦”ã♦”ã♦”ã♦Œççºèª♦ã♦•ã,Œã♦Ÿè£½å“♦

ä»—ã♦®ã,·ã,¹ã,³è£½å“♦ã♦«ã♦Šã♦,,ã♦|ã♦“ã,Œã,%oã♦®è,,†å¼±æ€§ã♦®å½±éŸ¿ã,’å♦—ã♦’ã,«ã

## è©³ç`°

Cisco Security Monitoring, Analysis and Response System(CS-

MARS)ã♦—ã€♦ã♦•ã♦³/4ã♦—ã♦³/4ã♦^ãf♦ãffãf^ãf¼ã,—ãf#ãf♦ã,¤ã,¹ã♦<ã,‰oã,¤ãf™ãf³ãf^ãfã,ºã,‘ã

MARSã♦—è‡ªå•ã,¿ã,¹ã,—ã,’å®Ÿè;Œã♦—ã♦|ã€♦ã,»ã,ãf¥ãf^ãftã,£ã♦®å•♦é;Œã,’è»½æ,›ã♦§ã♦?ã

- CS-

MARSã♦—Oracleãf#ãf¼ã,¿ãf™ãf¼ã,¹ã,’ä½¿ç”“ã♦—ã♦|ã€♦æ©Ÿå—tã♦®ãf♦ãffãf^ãf^ãf¼ã,—ã,

MARSã,çãf—ãf©ã,¤ã,çãf³ã,¹ã♦—ã€♦ãf#ãf¼ã,¿ãf™ãf¼ã,¹ã♦,ã♦®ãfãf¼ã,«ãf«ã♦Šã,^ã♦³ãf^ãfç

MARSã,çãf—ãf^ã,±ãf¼ã,·ãf§ãf³ã—ã€♦ãf#ãf•ã,©ãf«ãf^ã♦®Oracleãf#ãf¼ã,¿ãf™ãf¼ã,¹ã,çã,«ã,

Bug ID [CSCsd16256](#)(ç™»éŒ2ãf^ãf¼ã,¶å°,ç”“)ã♦«è”“è¿•ã,Œã♦|ã♦,,ã♦³/4ã♦™ã€,

- CS-MARSã♦«ã♦—ã€♦JBoss

Webã,çãf—ãf^ã,±ãf¼ã,·ãf§ãf³ã,µãf¼ãf♦ã♦®ã,¤ãf³ã,¹ãf^ãf¼ãf«ã♦Œå♦«ã♦³/4ã,Œã♦|ã♦,,ã♦

JMXã,³ãf³ã,½ãf¼ãf«ã,’ä»«ã♦—ã♦|CS-MARSç®jç♦†è€...ã♦®æ”©é™♦ã♦§CS-

MARSã,çãf—ãf©ã,¤ã,çãf³ã,¹ã,Šã♦§ã»»æ,,♦ã♦®ã,·ã,§ãf«ã,³ãfžãf³ãf‰oã,’å®Ÿè;Œã♦™ã,«ã€♦ç%

Bug ID [CSCse47646](#)(ç™»éŒ2ãf^ãf¼ã,¶å°,ç”“)ã♦«è”“è½æ,Œã♦|ã♦,,ã♦³/4ã♦™ã€,

- CS-MARS

å>žé◆?¿ç-

ä;®æ£æ, ^ã♦¿ã, ½ãƒ•ãƒ^ã, |ã, §ã, ¢

ã,çäffäf—ã,°äf~äf<sup>1</sup>/4äf‰oã,’æ¤œè·Žä?™ã,<å`^ä?—ä€? <http://www.cisco.com/go/psirt>  
ã? “å¾Œç¶šã?®ã,çäf‰oãf?ã,¤ã,¶äfãã,,å?...§ã?—ã? |ã€?å•?éjŒã?®è§Fæ±°çŠ¶æ³?ã? “å®ã,  
½äf?ãf?ãf?1/4ã,~äf§äf?ã,’çç?èª?ã?—ã? |ã? ?ã?ã?ã?•ã? „ã?,ã?,

Technical Assistance

Center i¼^TAC i¼% o ã ¾ ã   Yã   - ¢ „ , ã , ç ã , „ , ã   Sã   „ , ã , < ã f j ã f   f t ã f Šã f   ã , 1  
ã f - ã f ã f   ã , x ã f € ã f ¼ ã   « ã   Šå • ã   „ , ã   ^ ã   » ã   ã   ã   ã   ã   ã   , ã   , ã   , ã   ,

CS-

CS-

MARS® Česká republika, s.r.o., Řečkova 10, 160 00 Praha 6, Česká republika

<http://www.cisco.com/cisco/web/download/index.html>

CS-

<http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars?psrtdcat20e2>

ä, ◊ æ£å^©ç"“ ä°ä¾◊ “ å...¬å¼◊ç™øèì “

Cisco PSIRT

ã♦§ã♦~ã€♦æœ¬ã,¢ãf‰oãf♦ã,¤ã,¶ãfªã♦«è~è¼‰oã♦•ã,Œã♦|ã♦,ã, è,,†å¼±æ€§ã♦®ã,♦æ£å^©ç

JBossã¢®è,,†å¼±æ€§([CSCse47646\(c™»éŒ'ãf|ãf¼ã,¶ã°,ç”“\)](#))ã¢“ã€¢Jon

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060719-mars>

æ”’è”,å±¥æ’

ãf <sup>a</sup> ãf“ã, ,ãf§ãf <sup>3</sup> 1.0	2006å¹’7æœ^19æ—¥	å^♦å›žå...¬é-<ãf <sup>a</sup> ãf <sup>a</sup> f¼ã, <sup>1</sup>
--	------------------	---

å^©ç”’è!♦ç’,,

æœ¬ã,¢ãf%oãf♦ã,¤ã,¶ãf<sup>a</sup>ã♦¬ç„jä¿♦è”¼ã♦®ã,,ã♦®ã♦”ã♦—ã♦|ã♦”æ♦♦ä¾ã♦—ã♦|ã♦Šã,Šã€  
æœ¬ã,¢ãf%oãf♦ã,¤ã,¶ãf<sup>a</sup>ã♦®æf...å±ã♦Šã,^ã♦³ãf<sup>a</sup>ãf<sup>3</sup>ã,¬ã♦®ä½¿ç””ã♦«é-çã♦™ã,«è²¬ä»»ã♦®ä,€  
ã♦¾ã♦Ýã€♦ã,·ã,¹ã,³ã♦¬æœ¬ãf%oã,ãf¥ãf;ãf<sup>3</sup>ãf^ã♦®å†...å®¹ã,’ä°^å‘Šã♦ªã♦—ã♦«å¤%oæ»ã♦—ã♦  
æœ¬ã,¢ãf%oãf♦ã,¤ã,¶ãf<sup>a</sup>ã♦®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”³ã,’æ-½ã♦—ã♦Ýå‘å♦^ã€♦å½“ç¤¾ã♦Œç®;ç♦  
ã♦”ã♦®ãf%oã,ãf¥ãf;ãf<sup>3</sup>ãf^ã♦®æf...å±ã♦¬ã€♦ã,·ã,¹ã,³è£½å“♦ã♦®ã,“ãf<sup>3</sup>ãf%oãf|ãf¼ã,¶ã,’å¬¾è±;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。