

Cisco Prime Network Control Systems Database Default Credentials Vulnerability

Advisory ID: cisco-sa-20130410-ncs

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-ncs/>

æ—¥æœ—èªžã «ã, ^ã, <æf...å ±ã ¯ã€è±èªžã «ã, ^ã, <ãžÿæ-†ã ®éžã...-å¼ã ºç»è³ã šã,ã,š

Revision 1.1

Last Updated 2013 July 2 16:03 UTC (GMT)

For Public Release 2013 April 10 16:00 UTC (GMT)

ç>®æ¬;

[è!ç´„](#)

[è©²å¼½‘è£¼½“](#)

[è©³ç´°](#)

[è,,†å¼±æ€šã,¹ã,³ã,çè©³ç´°](#)

[å¼½±éÿ;](#)

[ã,¼ãf•ãf^ã,|ã,šã,çãfãf¼ã,ãfšãf³ãšã,^ã³ã;®æf](#)

[åž�éçç-](#)

[ã;®æfæ^ã;ã,¼ãf•ãf^ã,|ã,šã,çã®å...¥æ%œ<](#)

[ã,æfã^©ç””ã°<ã¼ãã”å...-å¼ç™°è;”](#)

[ã”ã®éšçÿ¥ã®ã,¹ãf†ãf¼ã,ã,¹¼šFINAL](#)

[æf...å±é...ã;ç](#)

[æ>æ-°å±æ´](#)

[ã,ã,¹ã,³ã,»ã,ãf¥ãf^ãf†ã,æ%œ<é†](#)

è!ç´„

ãfãf¼ã,ãfšãf³ 1.1.1.24 ã,^ã,šã%ã®ã,¼ãf•ãf^ã,|ã,šã,çã,å®ÿè;Çã—ã|ã,ã, < Cisco Prime Network Control System NCS

ã,çãf—ãf©ã,ªã,çãf³ã,¹ã «ã¯ã€ãf†ãf•ã,©ãf«ãf^ã®ã,¯ãf-ãf†ãf³ã,ãf£ãf«ãšã½œæ^ã•ã,Çãf!ãf¼ã,¶

ã,çã,«ã,|ãf³ãf^ãÇã«ã¼ã,Çã¼ã™ã€æ”æ’fè€...ãÇã”ã®ã,çã,«ã,|ãf³ãf^ã,¹¼ç””ã—

ã”ã®è,,†å¼±æ€šã,èš£æ±°ã™ã,ã«ã¯ã,¼ãf•ãf^ã,|ã,šã,çã®ã,çãffãf—ã,°ãf-ãf¼ãf%œãÇã

ã,ã,¹ã,³ã¯ã”ã®è,,†å¼±æ€šã«ã¼ã†|ã™ã,ç,,ã,ÿã®ã,¼ãf•ãf^ã,|ã,šã,ç

Vulnerability Scoring

Systemi^{1/4}CVSSi^{1/4}%ã «ãÿ°ã ¥ã „ã ÿã,1ã,3ã,çã,'æ »ã¼ã—ã |ã „ã¼ã™ã€æœ-ã,»ã,ãfã,çãf%ããfã,ã,ã,¶ã,¶ãfãã Sã® CVSS ã,1ã,3ã,çã-ã€CVSS ãfããf¼ã,ãfããf³ 2.0
ã «ãÿ°ã ¥ã „ã |ã „ã¼ã™ã€æœ,

CVSS

ã-ã€è,,tã¼±æ€Sã®é±è|ã°|ã,'ç°ã"tã™ã,ã,,ã®ã Sã€ç·Sæ€¥æ€Sã Sã,^ã³ã³¼ã¿œ

ã,ã,1ã,3ã Sã-ã€ãÿ°æœ-è©·ã¼ã,1ã,3ã,çã¼^Base

Scorei^{1/4}%ã Sã,^ã³ç¼çS¶è©·ã¼ã,1ã,3ã,çã¼^Temporal

Scorei^{1/4}%ã,'æ¼ã»ã—ã|ã „ã¼ã™ã€ã,ã Sã®çæS~ã-ã"ã,æã,%ãã,'ç"ã „ã|ç°ãçfè©

Scorei^{1/4}%ã,'ç®—ã±ã—ã€è±ãè«ã®ãfããfãf^ãfãf¼ã,ã «ã Sãã,ã,è,,tã¼±æ€Sã®ã¼±éÿ

ã,ã,1ã,3ã-æ-ã®ãfããfã,ã S CVSS

ã «é-çã™ã,è¿½ã S æf...ã ±ã,'æ¼ã»ã—ã|ã „ã¼ã™ã€æœ,

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

ã¼ãÿã,ã,1ã,3ã Sã-ã€ã,ãfããfãf^ãfãf¼ã,ã «ã Sãã,ç°ãçfã¼±éÿã°|ã,'ç®—ã±ã™
CVSS è^ç®—ãf,,ãf¼ããf«ã,'æ-ã®ãfããfã,ã Sæ¼ã¼ã—ã|ã „ã¼ã™ã€æœ,

<http://tools.cisco.com/security/center/cvssCalculator.x/>

CSCtz30468 - Cisco Prime Network Control System Default Credentials for Database User					
Calculate the environmental score of					
CVSS Base Score - 7.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score - 6.2					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed
------------	--------------	-----------

CSCub54624 - Cisco Prime Network Control System Default Credentials Vulnerability					
Calculate the environmental score of					
CVSS Base Score - 7.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Partial
CVSS Temporal Score - 6.2					
Exploitability	Remediation Level		Report Confidence		
Functional	Official-Fix		Confirmed		

Summary:

This vulnerability is a remote denial of service (DoS) attack. It is caused by a buffer overflow in the Cisco Prime Network Control System (NCS) default credentials. The attack is triggered by sending a specially crafted request to the NCS. The impact is a partial denial of service, which can be mitigated by applying the official fix. The report confidence is confirmed.

References:

For more information, please refer to the following references:
 - Cisco Security Advisories, Responses, and Notices: <http://www.cisco.com/g...>
 - CVE-2014-3624: <https://cve.mitre.org/cve/2014/3624>
 - NVD: <https://nvd.nist.gov/vuln/detail/CVE-2014-3624>

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。