

Cisco Prime Collaboration

SQL Injection Vulnerability in Cisco Prime Collaboration



CVE-2020-3184

2020-05-20 16:00

Final

CVSS 6.7

No workarounds available

Cisco ID : CSCvs29296

SQL Injection Vulnerability in Cisco Prime Collaboration

Summary

Cisco Prime Collaboration is vulnerable to a SQL injection attack. The vulnerability is located in the database layer and allows an attacker to execute arbitrary SQL queries.

The vulnerability is caused by a lack of input validation in the database queries. An attacker can inject malicious SQL code into the input fields, which is then executed by the database.

The impact of this vulnerability is that an attacker can access sensitive data, modify data, and execute administrative operations on the database. This could lead to a complete compromise of the system.

For more information, please refer to the following link: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pcp-sql-inj-22Auwt66>

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pcp-sql-inj-22Auwt66

Cisco Prime Collaboration is vulnerable to a SQL injection attack. The vulnerability is located in the database layer and allows an attacker to execute arbitrary SQL queries.

ä;®æfæ,^ã,½ãf•ãf^ã,|ã,šã,ç

ãfªãfªãf¼ã,¹ã«ã»ã,,ã|ã®æf...ã±ã«é-çã—ã|ã¬ã€ãã"ã®ã,çãf%ããã,ã,¶ã,¶ãfªã
ã®è©³ç°ã,»ã,¬ã,·ãfšãf³ã,'ã,ç...šã—ã|ä,ã·ã,,ã€,

ä, æfã^©ç" ä°<ã¾ã ã...-ã¼ç™°è; "

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ãšã¬ã€æœ¬ã,çãf%ããã,ã,¶ã,¶ãfªã«è¬¼%ã·ã,çãã|ã,,ã,«è,,†ã¼±æ€

ã†°ã... ,

Cisco ã¬ã"ã®è,,†ã¼±æ€šã,'ã±ãšã™ã,ããÿã,ã« it.sec ã®ã,¬ãfªã,¹ãf^ãf• Gmbh
Rottermann ã«æ,,ÿè¬ã™ã,ãã"ã "ã,'æœ¬ãç¼ã¾ã™ã€,

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccp-sql-inj-22Auwt66>

æ”¹è”,ã±ÿæ´

ã€”

ãfªãf¼ã,ãfšãf³	èª¬æž	ã,»ã,¬ã,·ãfšãf³	ã,¹ãf†ãf¼ã,çã,¹	Date
1.0	ã^ã>žã...-é-<ãfªãfªãf¼ã,¹		æœ¬€çç%ã^	2020-MAY-20

ã^©ç”è!ç´,,

æœ¬¬ã,çãf%ããã,ã,¶ã,¶ãfªã¬ç,,ãçèè¼ã®ã,,ã®ã"ã—ã|ã"æªªã¾ã—ã|ãšã,šã€
æœ¬¬ã,çãf%ããã,ã,¶ã,¶ãfªã®æf...ã±ãšã,ãã³ãfªãf³ã,¬ã®ã¼çç"ã«é-çã™ã,«è²¬ã»ã®ã,€
ã¾ãÿãÿã€ã,ã,¹ã,³ã¬æœ¬¬ãf%ãã,ãfªãfªãf³ãf^ã®ã†...ã®¹ã,'ã^ãšãªã—ã«ã%ãæ´ã—ã
æœ¬¬ã,çãf%ããã,ã,¶ã,¶ãfªã®è¬èç°ã†...ã®¹ã«é-çã—ã|æf...ã±é...ãç¼ã® URL
ã,çœçç·ã—ã€ããçç¬ã®è»çè¼%ã,,æ,,è³ã,'æ¬½ã—ãÿã´ã^ã€ã½"ç¾¾ãçççççç
ã"ã®ãf%ãã,ãfªãfªãf³ãf^ã®æf...ã±ã¬ãã,ã,¹ã,³è£½ã"ã®ã,¬ãf³ãf%ããã!ãf¼ã,¶ã,ã¼è±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。