

Cisco Common Services Platform

Collector (CSPC) Web API



Cisco Common Services Platform (CSPC) Web API : [CVE-2021-](#)

info-disc-KM3bGVL

[34774](#)

Published: 2021-11-03 16:00

Updated: 2022-01-06 17:54

Version: 1.1 : Final

CVSS Score: [4.9](#)

Workarounds: No workarounds available

Cisco ID: [CSCvz05854](#)

Collector (CSPC) Web API (CVE-2021-34774) - Medium Severity

Summary

Cisco Common Services Platform

Collector (CSPC) Web API (CVE-2021-34774) - Medium Severity

The vulnerability is located in the Collector (CSPC) Web API, which is used to manage the CSPC configuration.

The vulnerability is a Denial of Service (DoS) attack, which can be triggered by sending a large number of requests to the API.

The vulnerability is caused by a buffer overflow in the API, which can be triggered by sending a large number of requests.

For more information, please refer to the [Cisco Security Advisory](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-info-disc-KM3bGVL).

Impact

Denial of Service (DoS)

The vulnerability can be triggered by sending a large number of requests to the API.

The impact of the vulnerability is a Denial of Service (DoS) attack, which can be triggered by sending a large number of requests to the API.

The vulnerability is caused by a buffer overflow in the API, which can be triggered by sending a large number of requests.

The vulnerability is a Denial of Service (DoS) attack, which can be triggered by sending a large number of requests to the API.

The impact of the vulnerability is a Denial of Service (DoS) attack, which can be triggered by sending a large number of requests to the API.

The vulnerability is caused by a buffer overflow in the API, which can be triggered by sending a large number of requests.

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。