

Cisco SD-WAN

vManage Remote Code Execution (RCE) via Directory Traversal



Cisco Security Advisory ID : cisco-sa-

[CVE-2021-](#)

vman-dir-trav-Bpwc5gtm

[1465](#)

Published : 2021-03-03 16:00

Version : 1.0 : Final

CVSS Score : [4.3](#)

Workarounds : No workarounds available

Cisco ID : [CSCvu28396](#)

Remote Code Execution (RCE) via Directory Traversal

Summary

Cisco SD-WAN

vManage, a web-based management interface for Cisco SD-WAN, is vulnerable to Remote Code Execution (RCE) via Directory Traversal.

The vulnerability is located in the `HTTP` endpoint.

The vulnerability is caused by a directory traversal attack that allows an attacker to execute arbitrary code on the target system.

The vulnerability is caused by a directory traversal attack that allows an attacker to execute arbitrary code on the target system.

The vulnerability is caused by a directory traversal attack that allows an attacker to execute arbitrary code on the target system.

The vulnerability is caused by a directory traversal attack that allows an attacker to execute arbitrary code on the target system.

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-dir-trav-Bpwc5gtm>

References

1. [Cisco Security Advisory: Cisco SD-WAN vManage Remote Code Execution \(RCE\) via Directory Traversal](#)

2. [Cisco Security Advisory: Cisco SD-WAN vManage Remote Code Execution \(RCE\) via Directory Traversal](#)

- 18.4.6
- 19.2.4
- 20.1.2
- 20.3.2
- 20.4.1

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。