

# Cisco Modeling Labs Web UI


**High Severity CVE-2021-1531**



**CVE ID :** cisco-sa-cml- [CVE-2021-1531](#)  
**Command:** cmd-inject-N4VYeQXB  
**Published:** 2021-05-19 16:00  
**Version:** 1.0 : Final  
**CVSS Score:** [8.8](#)  
**Workarounds:** No workarounds available  
**Cisco ID:** [CSCvx78835](#)

**Summary:** A remote code execution vulnerability exists in the Cisco Modeling Labs Web UI.

## Impact

Cisco Modeling Labs  Web UI

The vulnerability allows an attacker to execute arbitrary code on the affected device via a specially crafted HTTP request.

Modeling Labs

The vulnerability exists in the `cmd-inject` endpoint of the `Web UI`.

The vulnerability is located in the `Web UI`.

The vulnerability is located in the `Web UI`.

The vulnerability is located in the `Web UI`.

Web UI

The vulnerability is located in the `Web UI`.

The vulnerability is located in the `Web UI`.

For more information, please refer to the following link:  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB>

## References

[https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB](#)





## 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。