

# Cisco Application Policy Infrastructure

## Controller, IP Address



**Medium**  **CVE-2020-3139**  
Cisco Application Policy Infrastructure (API) ID : cisco-sa-iptable-bypass-GxW88XjL

[CVE-2020-3139](#)

Published : 2020-01-22 16:00

Version : 1.0 : Final

CVSS Score : [5.3](#)

Workarounds : No workarounds available

Cisco ID : [CSCvs10135](#)

Summary of the vulnerability details.

### Impact

Cisco Application Policy Infrastructure

Controller (API) can be used to bypass the Out-of-Band (OOB) protection mechanism.

This vulnerability allows an attacker to bypass the OOB protection mechanism.

The vulnerability is present in the Cisco Application Policy Infrastructure (API) version 1.0.

For more information, please refer to the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iptable-bypass-GxW88XjL>

### References

1. [Cisco Security Advisory: Cisco Application Policy Infrastructure \(API\) OOB Protection Bypass](#)

2. [Cisco Security Advisory: Cisco Application Policy Infrastructure \(API\) OOB Protection Bypass](#)

3. [Cisco Security Advisory: Cisco Application Policy Infrastructure \(API\) OOB Protection Bypass](#)

4. [Cisco Security Advisory: Cisco Application Policy Infrastructure \(API\) OOB Protection Bypass](#)

5. [Cisco Security Advisory: Cisco Application Policy Infrastructure \(API\) OOB Protection Bypass](#)





## 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。