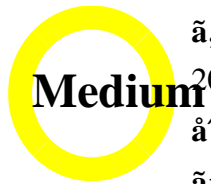


Cisco VPN Client for Windows



Severity: Medium
CVE ID: CVE-2018-0251
Product: Cisco VPN Client for Windows
Version: 5.0.0
CVSS Score: 6.1
Workarounds: No workarounds available
Cisco Bug ID: CSCvh20742

[CVE-2018-0251](#)

Summary: The Cisco VPN Client for Windows versions 5.0.0 and earlier are affected by a Denial of Service (DoS) vulnerability. An attacker can trigger a DoS attack by sending a specially crafted packet to the client.

Technical Details: The vulnerability is located in the Cisco VPN Client for Windows. It is triggered when a specially crafted packet is sent to the client.

Impact: The impact of this vulnerability is a Denial of Service (DoS) attack. An attacker can trigger a DoS attack by sending a specially crafted packet to the client.

Workarounds: No workarounds are available for this vulnerability.

References: [Cisco Security Advisory: Cisco VPN Client for Windows \(ASA\) Denial of Service Vulnerability](#)

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asawvpn2>

References

- 3000a, .afaf14a, °ç"£æçç"ª, »ã, ãfãfãftã, £ã, çãf—ãf©ã, mã, çãfãã, 1(ASA)ã, ½ãfãfã, |ã, šã, çã ©ã, ¯ãf©ã, mã, çãf³ Server Authentication Required)] ç"»é çã ©è,, tã¼±æ€šã «ã, ^ã, šã€è"è ¼ã •ã, Ćã |ã,, ããã,, ãfãfçãf¼ãf^ã ©æ"»æ'fè€..
- ã "ã ©è,, tã¼±æ€šã ¯ã€è"è ¼ã"ãfãfã, mã, 1ã ©Webãf™ãf¼ã, 1ã, mãf³ã, çãf¼ãfã, šã, mã, 1ã «ã, ^ã
- ã "ã ©è,, tã¼±æ€šã «ã ¾ã† |ã™ã, çãžé çç-ã ¯ã, ã, šã¾ã»ã, "ã€,,
- ã "ã ©ã, çãf%ãfã, mã, ¶ãfã ¯ã€æ-|ã ©ãfãfã, ¯ã, ^ã, šçç"èãã šããã¾ã™ã€,, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asawvpn2>

- [Cisco ASA 5500-X Security Advisories and Alerts](#)
- [Cisco Catalyst 6500 Security Advisories and Alerts](#)
- [Cisco 7600 Security Advisories and Alerts](#)

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

How to Report a Security Incident

1. Identify the affected device and the type of incident.

2. Report the incident

• Use the Cisco Bug ID or the Cisco Security Incident Response Center (CSIRC) portal.

3. Provide details of the incident

• Provide the following information:

• Bug ID (if known)
 • Device type and model
 • Software version
 • Configuration files
 • Logs and other relevant data

4. Wait for the response from the Cisco Security Incident Response Center (CSIRC). They will investigate the incident and provide you with the necessary information.

5. Follow the instructions provided by CSIRC to resolve the incident and prevent future occurrences.

6. Document the incident and the actions taken to resolve it. This will help you in the future and provide valuable information to the CSIRC.

7. Contact your local Cisco Technical Assistance Center (TAC) for further assistance.

How to Report a Security Incident

Cisco Product Security Incident Response

Team (PSIRT) will investigate the incident and provide you with the necessary information.

1. Identify the affected device

• Provide the following information:

• Device type and model
 • Software version
 • Configuration files
 • Logs and other relevant data

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。