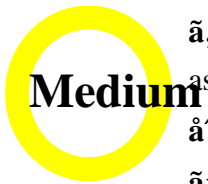


Cisco StarOS IPv6

Denial of Service (DoS) Vulnerability in Cisco StarOS IPv6



Severity: Medium
CVE ID: CVE-2020-3500
Product: Cisco StarOS IPv6
Version: 1.0 (Final)
CVSS Score: 6.8
Workarounds: No workarounds available
Cisco ID: CSCvu23797

[CVE-2020-3500](#)

Summary: A Denial of Service (DoS) vulnerability exists in Cisco StarOS IPv6. An attacker can exploit this vulnerability to cause a Denial of Service (DoS) attack on the device.

Impact

Cisco

StarOS IPv6 is vulnerable to a Denial of Service (DoS) attack. An attacker can exploit this vulnerability to cause a Denial of Service (DoS) attack on the device.

The vulnerability exists in the IPv6 stack.

The vulnerability is caused by a buffer overflow in the IPv6 stack.

The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device.

The vulnerability affects Cisco StarOS IPv6.

The vulnerability is present in Cisco StarOS IPv6 versions 1.0 and earlier.

The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device.

The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device.

The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-ipv6-dos-ce3zhF8m>

References

Cisco StarOS IPv6 Denial of Service (DoS) Vulnerability

The vulnerability exists in the IPv6 stack. The vulnerability is caused by a buffer overflow in the IPv6 stack. The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device. The vulnerability affects Cisco StarOS IPv6 versions 1.0 and earlier. The vulnerability can be exploited by sending a specially crafted IPv6 packet to the device.

æœ€ã,,åⓅæã...äøšæœ€æ-°äøæf...å ±äø«äøðäø,,äø|äø-äøäø"äøøã,çãf%øøãfäø,ðäø,¶äøãäø ID äøøèçç'°äø,»äø,äø,äøãfšãfäø,åø,ç...šãø—äø|äøäøäø äøøäø,,äø,

äø,äøæfå^©ç'"" äø<äø¾äøø " äø...-äø¼äøçTMøèj''

Cisco Product Security Incident Response

Teami¼PSIRTi¼%äø-äøæœ-äø,çãf%øøãfäø,ðäø,¶äøãäø«è""è¼%øøäøøäø,æãø|äø,,äø,è,,tä¼±æ€šãø

åø±øåø...,

äø"äøøè,,tä¼±æ€šãø- Cisco TAC

äø,µãfäøãf¼ãfäø,±ãf¼ãø,¹äøøèš€æ±øäø,äø«çTMøè|<äøøäø,æãø¾äøø—äøÿäø€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-ipv6-dos-ce3zhF8m>

æ''èø,å±ÿæ'

ãfäøãf¼ãø,ãfšãf³	èª-æž	ãø,»äø,äø,äøãfšãf³	äø,¹ãf±ãf¼ãø,çãø,¹	æ-ÿäø~
1.0	åø^äø>žåø...-é-ãfäøãf¼ãø,¹	-	Final	2020 å¹ 8 æœ^ 5 æ-ÿ

åø^©ç'""èè!çø,,

æœ-äø,çãf%øøãfäø,ðäø,¶äøãäøç,,jàçøè"¼ãøøãø,äøøãøø"äø—äø|äø"æøøøäø¾äø—äø|äøšãø,šãøæœ-äø,çãf%øøãfäø,ðäø,¶äøãäøøæf...å ±äøšäø,^äø³ãfäøãfäø,äøøà¼çç'"" äø«é-çäøTMäø,<è²-äø»äøøäø,äø¾äøøÿäø€äø,äø,¹äø,³äø-æœ-äøãf%øøãø,ãfãfãfãfäøøøäøøãøø...åø¹äø,äøø^äøšãøäøäø—äø«äøøøæ'äø—äøæœ-äø,çãf%øøãfäø,ðäø,¶äøãäøøè""èèçøåø...åøø¹äø«é-çäø—äø|æf...å ±é...äøçjãøø URL äø,çøøçøÿäø—äøäøäø~çø-äøøè»çè¼%øøäø,,æø,,èè³äø,æø-½äø—äøÿäø'äø^äø€äø½"çø¾äøøæçøççäøäø"äøøøãø,ãfãfãfãfäøøæf...å ±äø-äøäø,äø,¹äø,³èè½åø"äøøäø,äø"ãfãf%øøãf¼ãø,¶äø,åø¹äøèè¼è±j

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。