

Cisco Wireless LAN Controller (WLC) Denial of Service (DoS) Vulnerability



Severity: Medium
Product: Cisco Wireless LAN Controller (WLC)
Version: 7.4.110.0 and earlier
CVSS Score: 6.8
Workarounds: No Workarounds available
Cisco ID: CSCuh81011

[CVE-2013-6684](#)

Summary: A Denial of Service (DoS) vulnerability exists in the Cisco Wireless LAN Controller (WLC) software. An attacker can exploit this vulnerability to cause a denial of service on the WLC.

Details

Cisco Wireless LAN

Controller (WLC) software. The vulnerability is located in the `WLC` process.

The vulnerability is triggered when a specially crafted packet is sent to the WLC. The packet contains a malformed request that causes the WLC to crash.

The vulnerability is triggered when a specially crafted packet is sent to the WLC. The packet contains a malformed request that causes the WLC to crash.

The vulnerability is triggered when a specially crafted packet is sent to the WLC. The packet contains a malformed request that causes the WLC to crash.

The vulnerability is triggered when a specially crafted packet is sent to the WLC. The packet contains a malformed request that causes the WLC to crash.

References

For more information, see the following references:
Bug ID [CSCuh81011](#)

Workarounds

There are no workarounds available for this vulnerability. Cisco is working on a software fix.

ã¼ãÿã€ã,ã,¹ã³ãæœ-ãf%ã,ãfãfjãf³ãf^ã®ãt...ã®¹ã,'ã^ãšãªã—ã«ã%ãæ'ã—ã
æœ-ã,ããf%ããfãã,ãã,ããfãã®è"~è¿ãt...ã®¹ã«é-ãã—ã!æf...ã±é...ãã¿ãã® URL
ã,¿œ¿•ã—ã€ãã¿ã¿ã¿ã¿ã®è»¿è¼%ã,,æ,,è"³ã,'æ-½ã—ãÿã'ã^ã€ã½"¿ã¼ãã¿¿¿¿¿¿¿
ã"ã®ãf%ã,ãfãfjãf³ãf^ã®æf...ã±ãæ-ã,ã,¹ã,³è½ã"ã®ã,"ãf³ãf%ããf!ãf¼ã,ã,ã³¼è±jã

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。