

Cisco **WLC** LAN **DoS** Vulnerability 802.11 Denial of Service



CVE ID : cisco-sa-20180502-wlc-mfdos
Published : 2018-05-02 16:00
Updated : 2018-05-03 17:27
Version : Final
CVSS : [7.4](#)
Workarounds : No workarounds available
Cisco ID : [CSCvg07024](#)

[CVE-2018-0235](#)

Summary : A Denial of Service (DoS) vulnerability exists in Cisco Wireless LAN Controller (WLC) versions 7.5.2 through 8.5.3. An attacker can exploit this vulnerability by sending a specially crafted 802.11 management frame to the WLC, causing the WLC to crash and become unavailable to legitimate users.

Impact

Cisco Wireless LAN Controller (WLC) versions 7.5.2 through 8.5.3 are affected by a Denial of Service (DoS) vulnerability.

An attacker can exploit this vulnerability by sending a specially crafted 802.11 management frame to the WLC, causing the WLC to crash and become unavailable to legitimate users.

The vulnerability is rated as High (CVSS 7.4) because it can cause a Denial of Service (DoS) attack.

The vulnerability affects Cisco Wireless LAN Controller (WLC) versions 7.5.2 through 8.5.3.

The vulnerability is caused by a buffer overflow in the WLC's handling of 802.11 management frames.

The vulnerability is caused by a buffer overflow in the WLC's handling of 802.11 management frames.

The vulnerability is caused by a buffer overflow in the WLC's handling of 802.11 management frames.

For more information, see the Cisco Security Advisory <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-wlc-mfdos>.

References

è,,†â¼±æ€§ã®ã,ã,è£½â"◆

ã"ã®è,,†â¼±æ€§ã¬ã€Cisco Wireless LAN Controller ã,½ãfãf^ã,|ã,šã,ç ãfãfãf¼ã,¹
8.5.103.0 ã,â®ÿè;CEã—ã|ã,,ã,« Cisco Wireless LAN Controller
ã«ã½±éÿ;ã—ã¾ã™ã€,

è,,†â¼±æ€§ãCEã~ãœ"ã™ã,« Cisco WLC ã,½ãfãf^ã,|ã,šã,ç
ãfãfãf¼ã,¹ã®æf...ã ±ã«ã«ã,,ã|ã¬ã€ã"ã®ã,çãf%ãfã,ã,¶ã,¶ãfã®ãCEä;®æf

Cisco WLC ã,½ãfãf^ã,|ã,šã,ç ãfãfãf¼ã,¹ã®ã^ã¶

ãfãfãfã,ã,¹ãšã®ÿè;CEã•ã,CEã|ã,,ã,« Cisco WLC ã,½ãfãf^ã,|ã,šã,ç
ãfãfãf¼ã,¹ã¬ã€ç®;ç†è€...ãCEã,³ãfãf^ãfãf¼ãfã® Web
ã,ããfã,çãf¼ãfã,šã,ã,¹ã¾ãÿã¬ CLI
ã,'ã½ç"ã—ã|çç°èªã™ã,ãã"ã"ãCEãšãã¾ã™ã€,

Web ã,ããfã,çãf¼ãfã,šã,ã,¹ã,'ã½ç"ã™ã,ãã'ã^ã¬ã€æ¬ã,ã®ÿè;CEã—ã¾ã™ã€,

1. ãfãfã,ã,¶ã,¹ãšã®ÿè;CEã"ã,³ãfãf^ãfãf¼ãfã® Web
ã,ããfã,çãf¼ãfã,šã,ã,¹ã«ãfã,ã,ããfã—ã¾ã™ã€,
2. [ãfçãfã,çi¼^Monitori¼%] ã,çãfã,ã,ã,ãfãfã,ã—ã¾ã™ã€,
3. ããfãšã,ããfãšã€[Summaryi¼ã,ãfãfãfãi¼%] ã,ã,ãfãfãfã,ã—ã¾ã™ã€,
4. [ã,³ãfãf^ãfãf¼ãfã®ã,ãfãfãfãi¼^Controller Summaryi¼%] ã®ã,ã«ã,ã,
[ã,½ãfãf^ã,|ã,šã,çãfãf¼ã,ãfãfãf¼^Software Versioni¼%]
ãfã,£ãf¼ãf«ãf%ã«ã€ãfãfãfã,ã,¹ãšç¾ãœ"ã®ÿè;CEã•ã,CEã|ã,,ã,ã,½ãfãf^ã,|ã,šã,ç

CLI ã,'ã½ç"ã™ã,ãã'ã^ã¬ã€Telnet

ã,'ã½ç"ã—ã|ã,³ãfãf^ãfãf¼ãfã®ã«ãfã,ã,ããfã—ã|ã€show sysinfo
ã,³ãfãfãfãf%ã,ã®ÿè;CEã—ã€ã¶°ãšçµæžœã® Product Version
ãfã,£ãf¼ãf«ãf%ã®ã€ã,ã,ç...šã—ã¾ã™ã€,ãÿã"ã^ã°ãfãfãfã,ã,¹ãCE
Cisco WLC ã,½ãfãf^ã,|ã,šã,ç ãfãfãf¼ã,¹ 8.3.102.0
ã,ã®ÿè;CEã—ã|ã,,ã,ãã'ã^ã¬ã€ã,³ãfãfãfãf%ã®ã¶°ãšã¬æ¬ã®ã,ãã†ã«ãã,šã

<#root>

(wlc)>

show sysinfo

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version.....

8.3.102.0

◆<ã,‰œç>’æŽ¥è³¼å...¥ã◆—ã◆ÿã◆Ⓒ Cisco Service Contract

ã,ã◆”ã^©ç””ã◆,,ã◆ÿã◆ã◆,,ã◆|ã◆,,ã◆ã◆ã◆,,ã’ã◆^ã◆€◆ã◆³¼ã◆ÿã◆€◆ã,µãf¼ãf‰ãfãf¼ãftã,£ãf™

POSã◆<ã,‰œå...¥æ‰œ<ã◆šã◆◆ã◆ã◆ã◆,,ã’ã◆^ã◆—ã◆€◆Cisco TAC

ã◆«é€£çµjã◆—ã◆|ã,çãffãf—ã,°ãf-ãf¼ãf‰ã,ã’ã...¥æ‰œ<ã◆—ã◆|ã◆◆ã◆ã◆ã◆•ã◆,,ã€,

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

ç,,jã,,ÿã,çãffãf—ã,°ãf-ãf¼ãf‰ã◆®ã³¼è±jè£½ã”ã◆šã◆,ã,ã◆”ã◆”ã,è”¼æ~Žã◆—ã◆|ã◆,,ã◆ÿã◆

URLã,ã◆”ç””æ,,ã◆ã◆ã◆ã◆ã◆ã◆ã◆,,ã€,

ä;®æ£æ,^ã◆¿ãfãfãf¼ã,¹

ã,«ã,¹ã,¿ãfžãf¼ã◆—ã◆ã◆ã◆”ã◆®ã,»ã,—ã,ãfšãf³ã◆®èj”ã◆«æ²¿ã◆£ã◆|ã◆€◆é◆©ã^†ã◆ãfãfãf¼ã,

ã,½ãfãfãf¼ã,ãfšãf³ã,çç°èã◆ã◆—ã◆|ã◆◆ã◆ã◆ã◆ã◆•ã◆,,ã€,

- [cisco-sa-20180502-aironet-ssh](#):Cisco Aironet
1800ã◆€◆2800ã€◆ã◆šã,^ã◆³3800ã,ãfãf¼ã,°ã,çã,—ã,»ã,¹ãfã,µãf³ãf^ã◆®ã,»ã,ãfãã,çã,ã,šãf<
- [cisco-sa-20180502-ap-ptp](#):Cisco Aironet
1810ã◆€◆1830ã€◆ã◆šã,^ã◆³1850ã,ãfãf¼ã,°ã,çã,—ã,»ã,¹ãfã,µãf³ãf^ã◆®Point-to-Point Tunneling Protocol(PPTP)ã◆«ã◆šã◆’ã,«DoSè,,†ã¼±æ€š
- [cisco-sa-20180502-wlc-ip](#):Cisco Wireless LAN Controller IP Fragment Reassembly Denial of Service Vulnerability
- [cisco-sa-20180502-wlc-mfdos](#):Cisco Wireless LAN Controller
802.11ç®jç◆†ãfãf-ãf¼ãfã◆®Denial of Service(DoS)ã◆®è,,†ã¼±æ€š

æ¬jã◆®èj”ã◆šã◆—ã◆ã◆ã’ã◆®ã^—ã◆«ã,ã,¹ã,³ã,½ãfãfãfã,|ã,šã,çã◆®ãfjã,ãf£ãf¼

ãfãfãf¼ã,¹ã,çç°ã◆—ã◆³¼ã◆™ã€,,ã,ã®ã◆®ã^—ã◆Ⓒçç°ã◆™ã◆®ã◆—ã◆æœ—ã,çãf‰œã◆ã,µã,

ãfãfãf¼ã,¹ã◆,ã◆®ã½±éÿ¿ã◆®æœ‰œç,,jã◆€◆ã◆³¼ã◆ÿã◆€◆æœ—è,,†ã¼±æ€šã◆«ã³¼ã◆™ã,ã;®æ£æ

ãfãfãf¼ã,¹ã◆šã◆™ã€,,ã◆³ã◆®ã^—ã◆—ã◆—ã◆ãfjã,ãf£ãf¼

ãfãfãf¼ã,¹ã◆Ⓒã◆”ã◆®ã,³ãf-ã,—ã,ãfšãf³ã◆®ã,çãf‰œã◆ã,µã,¶ãfã◆«è”è¼‰œã◆—ã◆ÿã½ã,‰œ

<p>Cisco ãfã,µãfãf-ã,¹ LAN ã,³ãf³ãf^ãfãf¼ãf©ã◆”ã◆®è,,†ã¼±æ€šã◆«ã³¼ã◆™ã,æœœã^ã◆®ã;®æ£æãfãfãf¼ã,¹ ãfjã,ãf£ãf¼ ã,½ãfãfãfã,¹ã,šã,ç ãfãfãf¼ã,¹</p>	<p>ã◆”ã◆®è,,†ã¼±æ€šã◆«ã³¼ã◆™ã,æœœã^ã◆®ã;®æ£æãfãfãf¼ã,¹</p>	<p>First F for All Vulner Descri Collect Adviso</p>
<p>Prior to 8.0</p>	<p>è,,†ã¼±æ€šã◆ã◆—</p>	<p>è,,†ã¼±æ€šã◆</p>
<p>8.0</p>	<p>è,,†ã¼±æ€šã◆ã◆—</p>	<p>è,,†ã¼±æ€šã◆</p>
<p>8.1</p>	<p>è,,†ã¼±æ€šã◆ã◆—</p>	<p>è,,†ã¼±æ€šã◆</p>
<p>8.2</p>	<p>è,,†ã¼±æ€šã◆ã◆—</p>	<p>8.5.120</p>

8.3	è,,†â¼±æ€§ãªã—	8.5.120
8.4	è,,†â¼±æ€§ãªã—	8.5.120
8.5	è©²â¼²“ã€8.5.105.0ã«çš»èj€	8.5.120
8.6	è,,†â¼±æ€§ãªã—	è,,†â¼±æ€§ãªã—
8.7	è,,†â¼±æ€§ãªã—	è,,†â¼±æ€§ãªã—

ã,æfâ^©ç”” ä°<ã¾<ã”” å...-å¼ç™ºèj”

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ãª—ã€æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãª«è”~è¼%ãª•ã,€ãª |ãª,,ã,è,,†â¼±æ€§ãªª—

ãª°ã... ,

ãª“ãª®è,,†â¼±æ€§ãªª— Cisco TAC

ã,µãfãªf¼ãf^ã,±ãf¼ã,¹ãª®èš£æ±°ã,ãª«ç™ºè |ãª•ã,€ãª¾ãª—ãªÿã€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-wlc-mfdos>

æ”¹è””,ã±ÿæ´

ãfãªf¼ã,ãfšãf³	èª-æ~Ž
1.1	ã€€Cisco Mobility Express ã,½ãf•ãf^ã,ã,šã,çãªªã,ãª€Cisco Wireless LAN Controller ãª©ãª®ãªãªãªf¼ã,¹ãª® Cisco Mobility Express ã,½ãf•ãf^ã, ã,šã,çãªª€ãªfãªfãª,ãã,¹ãª®šã®ÿèj€ãª•ã,€ãªª ãª,,ã,ãªª,ãª^æª-
1.0	ãªª>ãªžã...-é-<ãªãªãªf¼ã,¹

ã^©ç””è|ç´,,

æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãªª—ç,,ãªçªè”¼ãª®ã,,ãª®ãªª—ãª—ãªª |ãª”æªªªª¾ãª—ãªª |ãªšã,šã€
æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãªª®æf...ã±ãªšã,^ãª³ãªãªãª,ãª®ã¼çç””ãª«é-çãª™ã,«è²-ãª»ãª®ã,€
ãª¾ãªÿãª€ãª,ã,¹ã,³ãªª—æœ-ãf%ãã,ãªãªfãªãªãªª®ãªª...ãª®¹ã,ãª°ãªšãªªãª—ãªª«ãª%ãªæ´ãª—ãªª
æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãªª®è”~èç°ãªª...ãª®¹ãª«é-çãª—ãªª |æf...ã±é...ªçjãª® URL
ã,çœªççª•ãª—ãª€ãªªª~ç<-ãª®è»çè¼%ãã,,æ,,ªè”³ã,æ-½ãª—ãªÿãªª^ãªªª½”çª¾ãªª€çç®jçª
ãªª“ãª®ãªf%ãã,ãªãªfãªãªãªª®æf...ã±ãªª—ãª€ãª,ã,¹ã,³è£½ãªªªª®ã,ãªãªãªf%ããf¼ã,¶ã,ãª¾è±ª

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。