

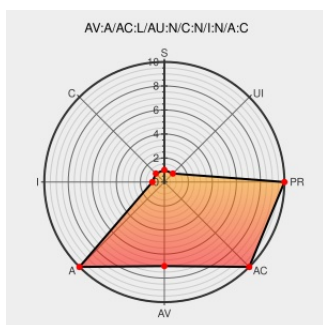


CVE-2015-0723

Published on: 05/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:18 PM UTC

CVE-2015-0723

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Wireless Lan Controller Software](#) from [Cisco](#) contain the following vulnerability:

The wireless web-authentication subsystem on Cisco Wireless LAN Controller (WLC) devices 7.5.x and 7.6.x before 7.6.120 allows remote attackers to cause a denial of service (process crash and device restart) via a crafted value, aka Bug ID CSCum03269.

CVE-2015-0723 has been assigned by [Cisco](#) [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **6.1 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Cisco Wireless LAN Controller Wireless Web Authentication Flaw Lets Remote Users Deny Service - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
[www.securitytracker.com](#)
[text/html](#)

[SECTrack 103227](#)

Cisco Wireless LAN Controller Wireless Web Authentication Denial of Service Vulnerability

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

[CISCO 20150508 Cisco Wireless LAN Controller Wireless Web Authentication Denial of Service Vulnerability](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Wireless Lan Controller Software	7.5.102.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	7.5.102.11	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	7.6.100.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	7.5.102.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	7.5.102.11	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	7.6.100.0	All	All	All
cpe:2.3:o:cisco:wireless_lan_controller_software:7.5.102.0:*****:.*:						
cpe:2.3:o:cisco:wireless_lan_controller_software:7.5.102.11:*****:.*:						
cpe:2.3:o:cisco:wireless_lan_controller_software:7.6.100.0:*****:.*:						
cpe:2.3:o:cisco:wireless_lan_controller_software:7.5.102.0:*****:.*:						
cpe:2.3:o:cisco:wireless_lan_controller_software:7.5.102.11:*****:.*:						
cpe:2.3:o:cisco:wireless_lan_controller_software:7.6.100.0:*****:.*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→