



# CVE-2022-20695

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-20695
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-15 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:42:00 UTC
<b>Description</b>	A vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthen

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	3504 Wireless Controller	-	All	All	All
Hardware	Cisco	5520 Wireless Controller	-	All	All	All
Hardware	Cisco	8540 Wireless Controller	-	All	All	All
Hardware	Cisco	Aironet 1540	-	All	All	All
Hardware	Cisco	Aironet 1542d	-	All	All	All
Hardware	Cisco	Aironet 1542i	-	All	All	All
Hardware	Cisco	Aironet 1560	-	All	All	All
Hardware	Cisco	Aironet 1562d	-	All	All	All
Hardware	Cisco	Aironet 1562e	-	All	All	All
Hardware	Cisco	Aironet 1562i	-	All	All	All
Hardware	Cisco	Aironet 1815	-	All	All	All
Hardware	Cisco	Aironet 1815i	-	All	All	All
Hardware	Cisco	Aironet 1815m	-	All	All	All
Hardware	Cisco	Aironet 1815t	-	All	All	All
Hardware	Cisco	Aironet 1815w	-	All	All	All
Hardware	Cisco	Aironet 1830	-	All	All	All
Hardware	Cisco	Aironet 1830e	-	All	All	All

Hardware	Cisco	Aironet 1830i	-	All	All	All
Hardware	Cisco	Aironet 1832	-	All	All	All
Hardware	Cisco	Aironet 1850	-	All	All	All
Hardware	Cisco	Aironet 1850e	-	All	All	All
Hardware	Cisco	Aironet 1850i	-	All	All	All
Hardware	Cisco	Aironet 1852	-	All	All	All
Hardware	Cisco	Aironet 2800	-	All	All	All
Hardware	Cisco	Aironet 2800e	-	All	All	All
Hardware	Cisco	Aironet 2800i	-	All	All	All
Hardware	Cisco	Aironet 3800	-	All	All	All
Hardware	Cisco	Aironet 3800e	-	All	All	All
Hardware	Cisco	Aironet 3800i	-	All	All	All
Hardware	Cisco	Aironet 3800p	-	All	All	All
Hardware	Cisco	Aironet 4800	-	All	All	All
Operating System	Cisco	Mobility Express Software	-	All	All	All
Application	Cisco	Virtual Wireless Controller	-	All	All	All
Hardware	Cisco	Virtual Wireless Controller	-	All	All	All
Application	Cisco	Wireless Lan Controller 8.10.151.0	All	All	All	All
Application	Cisco	Wireless Lan Controller 8.10.162.0	All	All	All	All

## References

Reference	Source	Link	Tags
20220413 Cisco Wireless LAN Controller Management Interface Authentication Bypass Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[317143](#) Cisco Wireless LAN Controller Management Interface Authentication Bypass Vulnerability (cisco-sa-wlc-auth-bypass-JRNhV4fF)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**