



# CVE-2018-0245

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

## Summary

<b>CVE</b>	CVE-2018-0245
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-02 22:29:00 UTC
<b>Updated</b>	2020-09-04 18:32:00 UTC
<b>Description</b>	A vulnerability in the REST API of Cisco 5500 and 8500 Series Wireless LAN Controller (WLC) Software could allow an unauthenticated user to obtain sensitive information from the target system.

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Wireless Lan Controller Software	8.3(133.0)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.3\133.0)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.5(105.0)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.5\105.0)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.3\133.0)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.5\105.0)	All	All	All

## References

### Reference

<a href="#">Cisco 5500 and 8500 Series Wireless LAN Controller Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System</a>
<a href="#">Cisco Wireless LAN Controller Software CVE-2018-0245 Information Disclosure Vulnerability</a>
<a href="#">Cisco 5500 and 8500 Series Wireless LAN Controller Information Disclosure Vulnerability</a>
<a href="#">CVE Program record</a>
<a href="#">NVD vulnerability detail</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

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