



# CVE-2018-0247

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

## Summary

<b>CVE</b>	CVE-2018-0247
<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>	2019-10-09 23:31:00 UTC
<b>Description</b>	A vulnerability in Web Authentication (WebAuth) clients for the Cisco Wireless LAN Controller (WLC) and Aironet Access P

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Aironet Access Point Software	8.3(104.105)	All	All	All
Operating System	Cisco	Aironet Access Point Software	8.3(104.105\)	All	All	All
Operating System	Cisco	Aironet Access Point Software	8.5(107.52)	All	All	All
Operating System	Cisco	Aironet Access Point Software	8.5(107.52\)	All	All	All
Operating System	Cisco	Aironet Access Point Software	8.3(104.105\)	All	All	All
Operating System	Cisco	Aironet Access Point Software	8.5(107.52\)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.3(104.105)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.3(104.105\)	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	8.3(104.105\)	All	All	All

## References

Reference	Source
Multiple Cisco Products CVE-2018-0247 Authentication Bypass Vulnerability	BID
Cisco Wireless LAN Controller WebAuth Bug Lets Remote Users Bypass Authentication on the Target Network - SecurityTracker	SECTRA
Cisco Aironet Access Points WebAuth Bug Lets Remote Users Bypass Authentication on the Target Network - SecurityTracker	SECTRA
Cisco Wireless LAN Controller and Aironet Access Points IOS WebAuth Client Authentication Bypass Vulnerability	CONFIRM
CVE Program record	CVE.ORG

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](#)