



# CVE-2018-0249

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2018-0249                                                                                                            |
| <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>         | 2020-10-22 16:46:00 UTC                                                                                                  |
| <b>Description</b>     | A vulnerability when handling incoming 802.11 Association Requests for Cisco Aironet 1800 Series Access Point (APs) on C |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                                       | Version    | Update | Edition | Language |
|------------------|-----------------------|-----------------------------------------------|------------|--------|---------|----------|
| Operating System | <a href="#">Cisco</a> | <a href="#">Aironet Access Point Software</a> | 8.2(161.0) | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Aironet Access Point Software</a> | 8.2\161.0\ | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Aironet Access Point Software</a> | 8.2\161.0\ | All    | All     | All      |

## References

| Reference                                                                                                          | Source   | Link                                    |
|--------------------------------------------------------------------------------------------------------------------|----------|-----------------------------------------|
| Cisco 1800 Series Aironet Access Points 802.11 AR Processing Flaw Lets Remote Users Deny Service - SecurityTracker | SECTrack | <a href="#">www.securitytracker.com</a> |
| Cisco Aironet 1800 Series Access Point 802.11 Denial of Service Vulnerability                                      | CONFIRM  | <a href="#">tools.cisco.com</a>         |
| CVE Program record                                                                                                 | CVE.ORG  | <a href="#">www.cve.org</a>             |
| NVD vulnerability detail                                                                                           | NVD      | <a href="#">nvd.nist.gov</a>            |

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)