# CVE-2017-12279

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-12279 |
| **State** | PUBLIC |
| **Assigner** | psirt@cisco.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-11-02 16:29:00 UTC |
| **Updated** | 2019-10-09 23:22:00 UTC |
| **Description** | A vulnerability in the packet processing code of Cisco IOS Software for Cisco Aironet Access Points could allow an unauthe |

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Cisco | Aironet Ap | - | All | All | All |
| Hardware | Cisco | Aironet Ap | - | All | All | All |
| Operating System | Cisco | Aironet Ap Firmware | - | All | All | All |
| Operating System | Cisco | Aironet Ap Firmware | - | All | All | All |

## References

| Reference |
|---|
| Cisco IOS Software for Cisco Aironet Access Points Information Disclosure Vulnerability |
| Cisco IOS for Cisco Aironet Access Points IP Packet Padding Error Lets Remote Users Obtain Potentially Sensitive Information on the Target |
| Cisco IOS Software for Aironet Access Points CVE-2017-12279 Information Disclosure Vulnerability |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

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