# CVE-2020-3560

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-3560 |
| **State** | PUBLIC |
| **Assigner** | psirt@cisco.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-09-24 18:15:00 UTC |
| **Updated** | 2021-04-16 15:01:00 UTC |
| **Description** | A vulnerability in Cisco Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of se |

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Cisco | 1111-4pwe | - | All | All | All |
| Hardware | Cisco | 1111-4pwe | - | All | All | All |
| Hardware | Cisco | 1111-8plteeawb | - | All | All | All |
| Hardware | Cisco | 1111-8plteeawb | - | All | All | All |
| Hardware | Cisco | 1111-8pwb | - | All | All | All |
| Hardware | Cisco | 1111-8pwb | - | All | All | All |
| Hardware | Cisco | 1113-8plteeawe | - | All | All | All |
| Hardware | Cisco | 1113-8plteeawe | - | All | All | All |
| Hardware | Cisco | 1113-8pmwe | - | All | All | All |
| Hardware | Cisco | 1113-8pmwe | - | All | All | All |
| Hardware | Cisco | 1113-8pwe | - | All | All | All |
| Hardware | Cisco | 1113-8pwe | - | All | All | All |
| Hardware | Cisco | 1116-4plteeawe | - | All | All | All |
| Hardware | Cisco | 1116-4plteeawe | - | All | All | All |
| Hardware | Cisco | 1116-4pwe | - | All | All | All |
| Hardware | Cisco | 1116-4pwe | - | All | All | All |
| Hardware | Cisco | 1117-4plteeawe | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Cisco | 1117-4plteeawe | - | All | All | All |
| Hardware | Cisco | 1117-4pmlteeawe | - | All | All | All |
| Hardware | Cisco | 1117-4pmlteeawe | - | All | All | All |
| Hardware | Cisco | 1117-4pmwe | - | All | All | All |
| Hardware | Cisco | 1117-4pmwe | - | All | All | All |
| Hardware | Cisco | 1117-4pwe | - | All | All | All |
| Hardware | Cisco | 1117-4pwe | - | All | All | All |
| Operating System | Cisco | Access Points | All | All | All | All |
| Operating System | Cisco | Access Points | All | All | All | All |
| Hardware | Cisco | Aironet 1542d | - | All | All | All |
| Hardware | Cisco | Aironet 1542d | - | All | All | All |
| Hardware | Cisco | Aironet 1542i | - | All | All | All |
| Hardware | Cisco | Aironet 1542i | - | All | All | All |
| Hardware | Cisco | Aironet 1562d | - | All | All | All |
| Hardware | Cisco | Aironet 1562d | - | All | All | All |
| Hardware | Cisco | Aironet 1562e | - | All | All | All |
| Hardware | Cisco | Aironet 1562e | - | All | All | All |
| Hardware | Cisco | Aironet 1562i | - | All | All | All |
| Hardware | Cisco | Aironet 1562i | - | All | All | All |
| Hardware | Cisco | Aironet 1815 | - | All | All | All |
| Hardware | Cisco | Aironet 1815 | - | All | All | All |
| Hardware | Cisco | Aironet 1830e | - | All | All | All |
| Hardware | Cisco | Aironet 1830e | - | All | All | All |
| Hardware | Cisco | Aironet 1830i | - | All | All | All |
| Hardware | Cisco | Aironet 1830i | - | All | All | All |
| Hardware | Cisco | Aironet 1850e | - | All | All | All |
| Hardware | Cisco | Aironet 1850e | - | All | All | All |
| Hardware | Cisco | Aironet 1850i | - | All | All | All |
| Hardware | Cisco | Aironet 1850i | - | All | All | All |
| Hardware | Cisco | Aironet 2800e | - | All | All | All |
| Hardware | Cisco | Aironet 2800e | - | All | All | All |
| Hardware | Cisco | Aironet 2800i | - | All | All | All |
| Hardware | Cisco | Aironet 2800i | - | All | All | All |
| Hardware | Cisco | Aironet 3800e | - | All | All | All |
| Hardware | Cisco | Aironet 3800e | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Cisco | Aironet 3800i | - | All | All | All |
| Hardware | Cisco | Aironet 3800i | - | All | All | All |
| Hardware | Cisco | Aironet 3800p | - | All | All | All |
| Hardware | Cisco | Aironet 3800p | - | All | All | All |
| Hardware | Cisco | Aironet 4800 | - | All | All | All |
| Hardware | Cisco | Aironet 4800 | - | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.1.2.6 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.1.2.9 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.2.0.37 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.10\(105.0\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.10\(105.4\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.5\(154.27\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.8\(125.0\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.1.2.6 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.1.2.9 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 17.2.0.37 | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.10\(105.0\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.10\(105.4\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.5\(154.27\) | All | All | All |
| Application | Cisco | Aironet Access Point Software | 8.8\(125.0\) | All | All | All |
| Hardware | Cisco | Business 140ac | - | All | All | All |
| Hardware | Cisco | Business 140ac | - | All | All | All |
| Hardware | Cisco | Business 145ac | - | All | All | All |
| Hardware | Cisco | Business 145ac | - | All | All | All |
| Hardware | Cisco | Business 240ac | - | All | All | All |
| Hardware | Cisco | Business 240ac | - | All | All | All |
| Application | Cisco | Business Access Points | All | All | All | All |
| Application | Cisco | Business Access Points | All | All | All | All |
| Hardware | Cisco | Catalyst 9105 | - | All | All | All |
| Hardware | Cisco | Catalyst 9105 | - | All | All | All |
| Hardware | Cisco | Catalyst 9115 | - | All | All | All |
| Hardware | Cisco | Catalyst 9115 | - | All | All | All |
| Hardware | Cisco | Catalyst 9117 | - | All | All | All |
| Hardware | Cisco | Catalyst 9117 | - | All | All | All |
| Hardware | Cisco | Catalyst 9120 | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Cisco | Catalyst 9120 | - | All | All | All |
| Hardware | Cisco | Catalyst 9130 | - | All | All | All |
| Hardware | Cisco | Catalyst 9130 | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-40 | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-40 | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-80 | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-80 | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-cl | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-cl | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l-c | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l-c | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l-f | - | All | All | All |
| Hardware | Cisco | Catalyst 9800-l-f | - | All | All | All |
| Hardware | Cisco | Catalyst Iw6300 | - | All | All | All |
| Hardware | Cisco | Catalyst Iw6300 | - | All | All | All |
| Hardware | Cisco | Esw-6300-con-x-k9 | - | All | All | All |
| Hardware | Cisco | Esw-6300-con-x-k9 | - | All | All | All |
| Operating System | Cisco | Wireless Lan Controller | All | All | All | All |
| Operating System | Cisco | Wireless Lan Controller | All | All | All | All |
| Operating System | Cisco | Wireless Lan Controller Software | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Cisco Aironet Access Points UDP Flooding Denial of Service Vulnerability | CISCO | tools.cisco.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**