



CVE-2010-0039

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2010-0039 |
| State | PUBLIC |
| Assigner | product-security@apple.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2010-12-22 03:00:00 UTC |
| Updated | 2011-01-19 06:53:00 UTC |
| Description | The Application-Level Gateway (ALG) on the Apple Time Capsule, AirPort Extreme Base Station, and AirPort Express Base |

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|----------|-----------------------|---|---------|--------|---------|----------|
| Hardware | Apple | Airport Express | All | All | All | All |
| Hardware | Apple | Airport Express | All | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 3.84 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 4.0.9 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 6.1 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 6.3 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 7.3.2 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 7.4.1 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 3.84 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 4.0.9 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 6.1 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 6.3 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 7.3.2 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | 7.4.1 | All | All | All |
| Hardware | Apple | Airport Express Base Station Firmware | All | All | All | All |
| Hardware | Apple | Airport Extreme | All | All | All | All |
| Hardware | Apple | Airport Extreme | All | All | All | All |

| | | | | | | |
|----------|-----------------------|---|-----|-----|-----|-----|
| Hardware | Apple | Airport Extreme Base Station Firmware | 5.5 | All | All | All |
| Hardware | Apple | Airport Extreme Base Station Firmware | 5.7 | All | All | All |
| Hardware | Apple | Airport Extreme Base Station Firmware | 5.5 | All | All | All |
| Hardware | Apple | Airport Extreme Base Station Firmware | 5.7 | All | All | All |
| Hardware | Apple | Time Capsule | All | All | All | All |
| Hardware | Apple | Time Capsule | All | All | All | All |

References

Reference

About the security content of Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2

SecurityTracker.com Archives - Apple Time Capsule and AirPort Base Station Bugs Let Remote Users Deny Service or Access Ostensibly Pro

APPLE-SA-2010-12-16-1 Time Capsule and AirPort Base Station (802.11n) Firmware 7.5.2

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.

© [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](#).

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