



# CVE-2014-8389

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

## Summary

<b>CVE</b>	CVE-2014-8389
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-28 02:29:03 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	cgi-bin/mft/wireless_mft.cgi in AirLive BU-2015 with firmware 1.03.18 16.06.2014, AirLive BU-3026 with firmware 1.43 21.08

## Risk And Classification

**Primary CVSS:** v3.0 9.8 CRITICAL from nvd@nist.gov

**CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

**Problem Types:** CWE-78 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	<b>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</b>
2.0	nvd@nist.gov	Primary	10		<b>AV:N/AC:L/Au:N/C/I:C/A:C</b>

## CVSS v3.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

**High**

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Airlive</a>	<a href="#">Bu-2015</a>	-	All	All	All
Operating System	<a href="#">Airlive</a>	<a href="#">Bu-2015 Firmware</a>	1.03.18_16.06.2014	All	All	All
Hardware	<a href="#">Airlive</a>	<a href="#">Bu-3026</a>	-	All	All	All
Operating System	<a href="#">Airlive</a>	<a href="#">Bu-3026 Firmware</a>	1.43_21.08.2014	All	All	All
Hardware	<a href="#">Airlive</a>	<a href="#">Md-3025</a>	-	All	All	All
Operating System	<a href="#">Airlive</a>	<a href="#">Md-3025 Firmware</a>	1.81_21.08.2014	All	All	All
Hardware	<a href="#">Airlive</a>	<a href="#">Poe-200cam V2</a>	-	All	All	All
Operating System	<a href="#">Airlive</a>	<a href="#">Poe-200cam V2 Firmware</a>	lm.1.6.17.01	All	All	All
Hardware	<a href="#">Airlive</a>	<a href="#">WI-2000cam</a>	-	All	All	All
Operating System	<a href="#">Airlive</a>	<a href="#">WI-2000cam Firmware</a>	lm.1.6.18_14.10.2011	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source	Link
Multiple AirLive Products Multiple OS Command Injection Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.sc</a>

AirLive Remote Command Injection ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	<a href="#">packetstorm</a>
AirLive Multiple Products OS Command Injection   CoreLabs Advisory	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.corelabs.com</a>
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.securityfocus.com</a>
Full Disclosure: [CORE-2015-0012] - AirLive Multiple Products OS Command Injection	af854a3a-2127-422b-91ae-364da2661108	<a href="#">seclists.org</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.

© [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](#)