

CVE-2010-5330

Ubiquiti AirOS Command Injection Vulnerability

CISA KEV since Apr 15, 2022

Actively exploited

On certain Ubiquiti devices, Command Injection exists via a GET request to stainfo.cgi (aka Show AP info) because the ifname variable is not sanitized, as demonstrated by shell metacharacters. The fixed version is v4.0.1 for 802.11 ISP products, v5.3.5 for AirMax ISP products, and v5.4.5 for AirSync firmware. For example, Nanostation5 (Air OS) is affected.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.402 98.6th percentile · FIRST	CISA DEADLINE May 6, 2022 KEV since 2022 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.402 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
airos	< 4.0.1 ≥ 4.0.2 < 5.3.5 ≥ 5.3.6 < 5.4.5	4.0.1 · 5.3.5 · 5.4.5	NVD

Sources

Vendor guidance	community.ubnt.com/t5/airMAX-General-Discussion/AirOS-Security-Exploit-Updated-Firmware/td-p/212974	NVD	nvd.nist.gov/vuln/detail/CVE-2010-5330
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2010-5287
Current data	evulnable.com/vulnerability-management/cve/CVE-2010-5330		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.