



CVE-2013-0134

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

Summary

CVE	CVE-2013-0134
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-09 03:34:53 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the web interface in AirDroid allows remote attackers to inject arbitrary web script

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Airdroid	Airdroid	-	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	Ta
Vulnerability Note VU#557252 - AirDroid web interface XSS vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.kb.cert.org	US
CVE Program record	CVE.ORG		www.cve.org	ca
NVD vulnerability detail	NVD		nvd.nist.gov	ca
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				