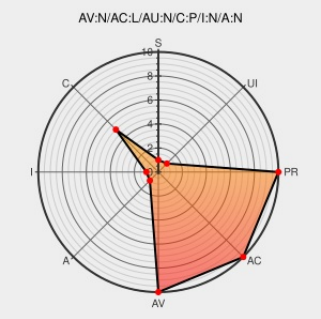
CVE-2012-3886

Published on: 07/26/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:16 PM UTC

CVE-2012-3886

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Airdroid from Airdroid contain the following vulnerability:

AirDroid 1.0.4 beta uses the MD5 algorithm for values in the checklogin key parameter and 7bb cookie, which makes it easier for remote attackers to obtain cleartext data by sniffing the local wireless network and then conducting a (1) brute-force attack or (2) rainbow-table attack.

CVE-2012-3886 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
	Exploit, www.tele-consulting.com, text/plain	MISC www.tele-consulting.com/advisories/TC-SA-2012-02.txt
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20120712 security advisory: AirDroid 1.0.4 beta

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Airdroid	Airdroid	1.0.4	beta	All	All
Application	Airdroid	Airdroid	1.0.4	beta	All	All

cpe:2.3:a:airdroid:airdroid:1.0.4:beta:*:*:*:*:*:*:

cpe:2.3:a:airdroid:airdroid:1.0.4:beta:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→