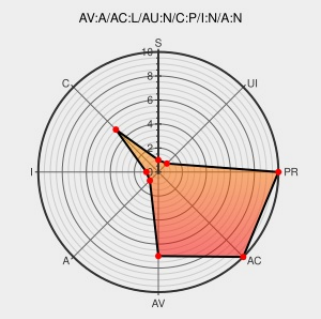
CVE-2015-5853

Published on: 10/08/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5853

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



Certain versions of Mac Os X from Apple contain the following vulnerability:

AirScan in Apple OS X before 10.11 allows man-in-the-middle attackers to obtain eSCL packet payload data via unspecified vectors.

CVE-2015-5853 has been assigned by product-security@apple.com to track the vulnerability

CVSS2 Score: 3.3 - LOW

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

CVE References

Description	Tags	Link
Apple OS X Multiple Flaws Let Remote and Local Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Deny Service and Let Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1033703
APPLE-SA-2015-09-30-3 OS X El Capitan 10.11	Vendor Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2015-09-30-3
About the security content of OS X El Capitan v10.11 - Apple Support	Vendor Advisory, support.apple.com, text/html	CONFIRM support.apple.com/HT205267

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→