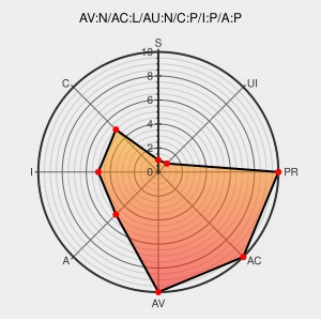
CVE-2014-1262

Published on: 02/26/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-1262

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



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

Apple Type Services (ATS) in Apple OS X before 10.9.2 allows attackers to bypass the App Sandbox protection mechanism via crafted Mach messages that trigger memory corruption.

CVE-2014-1262 has been assigned by product-security@apple.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
About the security content of OS X Mavericks v10.9.2 and Security Update 2014-001 - Apple Support	Vendor Advisory, support.apple.com, text/html	CONFIRM support.apple.com/kb/HT6150

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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	10.9	All	All	All
Operating System	Apple	Mac Os X	10.9	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

cpe:2.3:o:apple:mac_os_x:10.9:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.9:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→