



CVE-2013-3949

Published on: 06/05/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

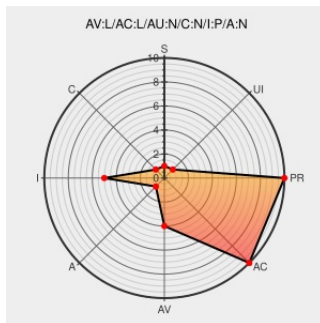
CVE-2013-3949

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

The posix_spawn system call in the XNU kernel in Apple Mac OS X 10.8.x does not prevent use of the _POSIX_SPAWN_DISABLE_ASLR and _POSIX_SPAWN_ALLOW_DATA_EXEC flags for setuid and setgid programs, which allows local users to bypass intended access restrictions via a wrapper program that calls the posix_spawnattr_setflags function.

CVE-2013-3949 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

SyScan'14
Singapore -
Day 2 (4th
April 2014)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

[MISC](#) [www.syscan.org/index.php/sg/program/day/2](#)

404 - Not
Found

[Exploit](#)

[antid0te.com](#)

[application/pdf](#)

[Inactive Link](#)

[Not Archived](#)

[MISC](#)

[antid0te.com/syscan_2013/SyScan2013_Mountain_Lion_iOS_Vulnerabilities_Garage_Sale_White](#)

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 warrant the accuracy of the information provided on these sites. CVEreport is not responsible for any damage or loss resulting from the use of the information provided on these sites.

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	10.8.0	All	All	All
Operating System	Apple	Mac Os X	10.8.1	All	All	All
Operating System	Apple	Mac Os X	10.8.2	All	All	All
Operating System	Apple	Mac Os X	10.8.3	All	All	All
Operating System	Apple	Mac Os X	10.8.4	All	All	All
Operating System	Apple	Mac Os X	10.8.0	All	All	All
Operating System	Apple	Mac Os X	10.8.1	All	All	All
Operating System	Apple	Mac Os X	10.8.2	All	All	All
Operating System	Apple	Mac Os X	10.8.3	All	All	All
Operating System	Apple	Mac Os X	10.8.4	All	All	All

cpe:2.3:o:apple:mac_os_x:10.8.0:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.1:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.2:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.3:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.4:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.0:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.1:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.2:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.3:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.8.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)