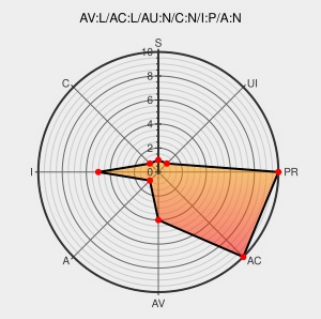
# CVE-2013-3949

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 cve@mitre.org to track the vulnerability

## CVSS2 Score: 2.1 - LOW

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | 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 |

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 | 10.8.0 | 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→