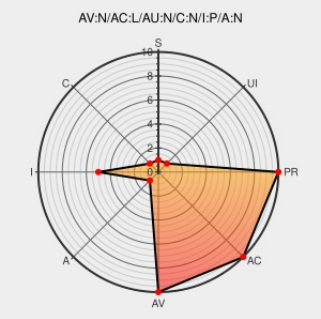
# CVE-2013-3950

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

Last Modified on: 03/23/2021 11:28:31 PM UTC

## CVE-2013-3950

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




Certain versions of Iphone Os from Apple contain the following vulnerability:

Stack-based buffer overflow in the openSharedCacheFile function in dyld.cpp in dyld in Apple iOS 5.1.x and 6.x through 6.1.3 makes it easier for attackers to conduct untethering attacks via a long string in the DYLD_SHARED_CACHE_DIR environment variable.

CVE-2013-3950 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** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| About the security content of iOS 7 | support.apple.com text/html | CONFIRM support.apple.com/kb/HT5934 |
| APPLE-SA-2013-10-22-3 OS X Mavericks v10.9 | lists.apple.com text/html | APPLE APPLE-SA-2013-10-22-3 |
| 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 Vendor Advisory | MISC antid0te.com/syscan_2013/SyScan2013_Mountain_Lion_iOS_Vulnerabilities_Garage_Sale_W |

| | | |
|---|---|---|
| | antid0te.com<br>application/pdf<br>Inactive Link Not Archived | |
| Apple iOS Multiple Bugs Let Remote Users Execute Arbitrary Code, Deny Service, Obtain Information, and Conduct Cross-Site Scripting Attacks and Let Applications Gain Elevated Privileges - SecurityTracker | www.securitytracker.com<br>text/html | SECTRACK 1029054 |
| APPLE-SA-2013-09-18-2 iOS 7 | lists.apple.com<br>text/html | APPLE APPLE-SA-2013-09-18-2 |



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 | Iphone Os | 5.1 | All | All | All |
| Operating System | Apple | Iphone Os | 5.1.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0.2 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1.2 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1.3 | All | All | All |
| Operating System | Apple | Iphone Os | 5.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Apple | Iphone Os | 5.1.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.0.2 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1.2 | All | All | All |
| Operating System | Apple | Iphone Os | 6.1.3 | All | All | All |

cpe:2.3:o:apple:iphone_os:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:6.1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**