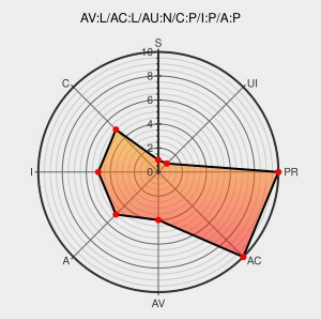
CVE-2013-3951

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

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

CVE-2013-3951

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



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

sys/openbsd/stack_protector.c in libc in Apple iOS 6.1.3 and Mac OS X 10.8.x does not properly parse the Apple strings employed in the user-space stack-cookie implementation, which allows local users to bypass cookie randomization by executing a program with a call-path beginning with the stack-guard= substring, as demonstrated by an iOS untethering attack or an attack against a setuid Mac OS X program.

CVE-2013-3951 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
APPLE-SA-2015-09-16-1 iOS 9	Vendor Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2015-09-16-1
Apple OS X Multiple Flaws Let Remote and Local Users Execute Arbitrary Code, Obtain Potentially Sensitive	www.securitytracker.com, text/html	SECTRACK 1033703

Information, and Deny Service and Let Local Users Gain Elevated Privileges - SecurityTracker		
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 watchOS 2 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT205213
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
About the security content of iOS 9 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT205212
404 - Not Found	Exploit antid0te.com application/pdf Inactive Link Not Archived	MISC antid0te.com/syscan_2013/SyScan2013_Mountain_Lion_iOS_Vulnerabilities_Garage_Sale_W
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
APPLE-SA-2015-09-21-1 watchOS 2	Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2015-09-21-1

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	6.1.3	All	All	All
Operating System	Apple	Iphone Os	6.1.3	All	All	All
Operating System	Apple	Iphone Os	All	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
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	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

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

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

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

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:*:*:*:*:*:*:*:

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

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→