



CVE-2016-1757

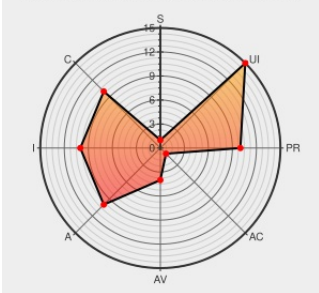
Published on: 03/23/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:05 PM UTC

CVE-2016-1757

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H



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

Race condition in the kernel in Apple iOS before 9.3 and OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context via a crafted app.

CVE-2016-1757 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002	Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-03-21-5
Apple Mac OSX / iOS - SUID Binary Logic Error Kernel Code Execution	www.exploit-db.com	EXPLOIT-DB 39595

	Proof of Concept text/html	
Exploit – Page 39741 – Exploits Database	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39741
About the security content of iOS 9.3 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206166
676 - Logic error when exec-ing suid binaries allows code execution as root on OS X/iOS - project-zero - Monorail	bugs.chromium.org text/html	 MISC bugs.chromium.org/p/project-zero/issues/detail?id=676
APPLE-SA-2016-03-21-1 iOS 9.3	Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-03-21-1
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Remote and Local Users Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1035353
About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206167

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

Exploit/POC from Github

Exploit code for CVE-2016-1757

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
cpe:2.3:o:apple:iphone_os:*****:.*:						
cpe:2.3:o:apple:mac_os_x:*****:.*:						

No vendor comments have been submitted for this CVE

© [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](#)