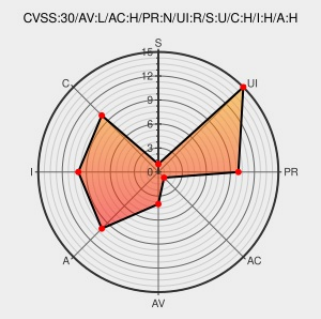
CVE-2016-1757

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



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	SECTRACK 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

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

← Previous ID

Next ID→

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