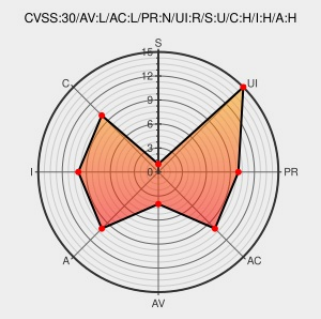
CVE-2016-4698

Published on: 09/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:58 PM UTC

CVE-2016-4698

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



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

AppleMobileFileIntegrity in Apple iOS before 10 and OS X before 10.12 mishandles process entitlement and Team ID values in the task port inheritance policy, which allows attackers to execute arbitrary code in a privileged context via a crafted app.

CVE-2016-4698 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	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-2016-09-20-3 iOS 10	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-09-20-3

About the security content of macOS Sierra 10.12 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT207170
Apple macOS/OS X Multiple Flaws Let Remote and Local Users Deny Service, Obtain Potentially Sensitive Information, Execute Arbitrary Code, and Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036858
APPLE-SA-2016-09-20 macOS Sierra 10.12	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-09-20
About the security content of iOS 10 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT207143
No Description Provided	cve.report (archive) text/html	BID 93056

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

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→