

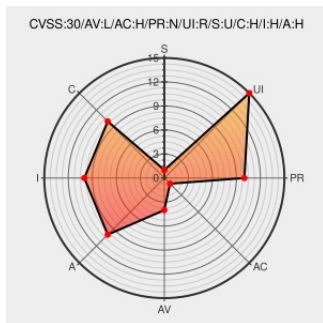


CVE-2017-7004

Published on: 04/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-7004

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

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

An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "Security" component. A race condition allows attackers to bypass intended entitlement restrictions for sending XPC messages via a crafted app.

CVE-2017-7004 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: **5.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
About the security content of iOS 10.3.2 - Apple Support	Vendor Advisory support.apple.com/text/html	CONFIRM support.apple.com/HT207798

About the security content of macOS Sierra 10.12.5, Security Update 2017-002 El Capitan, and Security Update 2017-002 Yosemite - Apple Support

Vendor Advisory

support.apple.com

text/html

CONFIRM

support.apple.com/HT207797

Apple macOS 10.12.3 / iOS < 10.3.2 - Userspace Entitlement Checking Race Condition - Multiple local Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

EXPLOIT-DB 42145

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	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	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:iphone_os:*****:*						
cpe:2.3:o:apple:mac_os_x:*****:*						
cpe:2.3:o:apple:mac_os_x:*****:*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →