

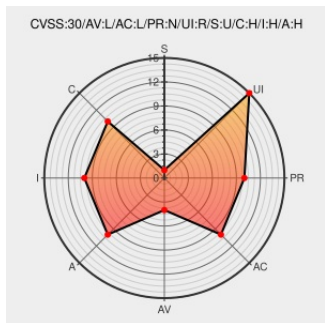


CVE-2018-4243

Published on: 06/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:16 PM UTC

CVE-2018-4243

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

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

An issue was discovered in certain Apple products. iOS before 11.4 is affected. macOS before 10.13.5 is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "Kernel" component. A buffer overflow in getvolattrlist allows attackers to execute arbitrary code in a privileged context via a crafted app.

CVE-2018-4243 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
1564 - MacOS/iOS kernel heap overflow due to lack of lower size check in getvolattrlist - project-zero - Monorail	Exploit Issue Tracking Third Party Advisory	MISC bugs.chromium.org/p/project-zero/issues/detail?id=1564

bugs.chromium.org
[text/html](#)

About the security content of tvOS 11.4 - Apple Support

[Vendor Advisory](#)
support.apple.com
[text/html](#)

 **CONFIRM**
support.apple.com/HT208850

Apple macOS/OS X Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Local Users Obtain Potentially Sensitive Information, Bypass Security, and Gain Elevated Privileges - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
www.securitytracker.com
[text/html](#)

 **SECURITYTRACKER** 1041027

About the security content of iOS 11.4 - Apple Support

[Vendor Advisory](#)
support.apple.com
[text/html](#)

 **CONFIRM**
support.apple.com/HT208848

About the security content of watchOS 4.3.1 - Apple Support

[Vendor Advisory](#)
support.apple.com
[text/html](#)

 **CONFIRM**
support.apple.com/HT208851

Apple macOS/iOS Kernel - Heap Overflow Due to Lack of Lower Size Check in getvolattrlist - Multiple dos Exploit

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

 **EXPLOIT-DB** 44848

About the security content of macOS High Sierra 10.13.5, Security Update 2018-003 Sierra, Security Update 2018-003 El Capitan - Apple Support

[Vendor Advisory](#)
support.apple.com
[text/html](#)

 **CONFIRM**
support.apple.com/HT208849

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

empty_list - exploit for p0 issue 1564 (CVE-2018-4243) iOS 11.0 - 11.3.1 kernel r/w

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Apple Tv	All	All	All	All
Application	Apple	Apple Tv	All	All	All	All
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
Operating System	Apple	Watchos	All	All	All	All

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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