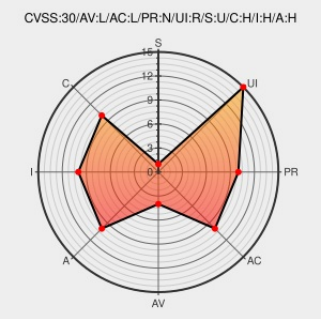
# CVE-2018-4243

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<br>Issue Tracking<br>Third Party Advisory | MISC<br>bugs.chromium.org/p/project-zero/issues/detail?id=1564 |

| | | |
|---|---|---|
| | bugs.chromium.org<br>text/html | |
| About the security content of tvOS 11.4 - Apple Support | Vendor Advisory<br>support.apple.com<br>text/html | CONFIRM<br>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<br>VDB Entry<br>www.securitytracker.com<br>text/html | SECTRACK 1041027 |
| About the security content of iOS 11.4 - Apple Support | Vendor Advisory<br>support.apple.com<br>text/html | CONFIRM<br>support.apple.com/HT208848 |
| About the security content of watchOS 4.3.1 - Apple Support | Vendor Advisory<br>support.apple.com<br>text/html | CONFIRM<br>support.apple.com/HT208851 |
| Apple macOS/iOS Kernel - Heap Overflow Due to Lack of Lower Size Check in getvolattrlist - Multiple dos Exploit | Exploit<br>Third Party Advisory<br>VDB Entry<br>www.exploit-db.com<br>Proof of Concept<br>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<br>support.apple.com<br>text/html | CONFIRM<br>support.apple.com/HT208849 |



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 | Apple | Watches | All | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Apple | Watchos | All | All | All | All |
| Operating System | Apple | Watchos | All | All | All | All |

cpe:2.3:a:apple:apple_tv:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:apple_tv:*:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→