



CVE-2018-4280

Published on: 04/03/2019 12:00:00 AM UTC

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

CVE-2018-4280

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

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

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 11.4.1, macOS High Sierra 10.13.6, tvOS 11.4.1, watchOS 4.3.2.

CVE-2018-4280 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: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
About the security content of tvOS 11.4.1 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/kb/HT208936
About the security content of iOS 11.4.1 - Apple Support	Vendor Advisory	MISC

About the security content of watchOS 4.3.2 - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC
support.apple.com/kb/HT208935

About the security content of macOS High Sierra 10.13.6, Security Update 2018-004
Sierra, Security Update 2018-004 El Capitan - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC
support.apple.com/kb/HT208937

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

CVE-2018-4280: Mach port replacement vulnerability in launchd on iOS 11.2.6 leading to sandbox escape, privilege esca...

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
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Apple	Watchos	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:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:
```

cpe:2.3:o:apple:tvos:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:apple:watchos:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:apple:watchos:*.*.*.*.*.*.*.*.*.*

```
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→

© CVE.report 2023 |

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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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