



CVE-2016-4718

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-4718
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-25 10:59:25 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Buffer overflow in FontParser in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted PDF documents, as demonstrated by the PoC exploit in the Apple Security Advisory. CVE-2016-4718 is a buffer overflow in the FontParser component of the CoreText framework in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3. The vulnerability allows a remote attacker to execute arbitrary code or cause a denial of service (memory consumption) via crafted PDF documents, as demonstrated by the PoC exploit in the Apple Security Advisory. CVE-2016-4718 is a buffer overflow in the FontParser component of the CoreText framework in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3. The vulnerability allows a remote attacker to execute arbitrary code or cause a denial of service (memory consumption) via crafted PDF documents, as demonstrated by the PoC exploit in the Apple Security Advisory.

Risk And Classification

Primary CVSS: v3.0 6.5 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

EPSS: 0.023200000 probability, percentile 0.848770000 (date 2026-05-06)

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

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
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
APPLE-SA-2016-09-20-5 watchOS 3
About the security content of iOS 10 - Apple Support
About the security content of tvOS 10 - Apple Support
About the security content of macOS Sierra 10.12 - Apple Support
About the security content of watchOS 3 - Apple Support
APPI F-SA-2016-09-20 macOS Sierra 10.12

APPLE-SA-2016-09-20-6 tvOS 10

Apple iOS/tvOS/macOS/watchOS Multiple Security Vulnerabilities

Apple macOS/OS X Multiple Flaws Let Remote and Local Users Deny Service, Obtain Potentially Sensitive Information, Execute Arbitrary Code

APPLE-SA-2016-09-20-3 iOS 10

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)