About the security content of iOS 11

This document describes the security content of iOS 11.

About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security updates page.

For more information about security, see the Apple Product Security page. You can encrypt communications with Apple using the Apple Product Security PGP Key.

Apple security documents reference vulnerabilities by CVE-ID when possible.

iOS 11

Released September 19, 2017

Bluetooth

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to access restricted files

Description: A privacy issue existed in the handling of Contact cards. This was addressed with improved state management.

CVE-2017-7131: an anonymous researcher, Elvis (@elvisimprsntr), Dominik Conrads of Federal Office for Information Security, an anonymous researcher

Entry added September 25, 2017

CFNetwork Proxies

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker in a privileged network position may be able to cause a denial of service

Description: Multiple denial of service issues were addressed through improved memory handling.

CVE-2017-7083: Abhinav Bansal of Zscaler Inc.

Entry added September 25, 2017

CoreAudio

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to read restricted memory

Description: An out-of-bounds read was addressed by updating to Opus version 1.1.4.

CVE-2017-0381: V.E.O (@VYSEa) of Mobile Threat Research Team, Trend Micro

Entry added September 25, 2017

Exchange ActiveSync

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker in a privileged network position may be able to erase a device during Exchange account setup

Description: A validation issue existed in AutoDiscover V1. This was addressed by requiring TLS for AutoDiscover V1. AutoDiscover V2 is now supported.

CVE-2017-7088: Ilya Nesterov, Maxim Goncharov

Heimdal

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker in a privileged network position may be able to impersonate a service

Description: A validation issue existed in the handling of the KDC-REP service name. This issue was addressed through improved validation.

CVE-2017-11103: Jeffrey Altman, Viktor Duchovni, and Nico Williams

Entry added September 25, 2017

iBooks

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Parsing a maliciously crafted iBooks file may lead to a persistent denial-of-service

Description: Multiple denial of service issues were addressed through improved memory handling.

CVE-2017-7072: Jędrzej Krysztofiak

Kernel

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2017-7114: Alex Plaskett of MWR InfoSecurity

Entry added September 25, 2017

Keyboard Suggestions

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Keyboard autocorrect suggestions may reveal sensitive information

Description: The iOS keyboard was inadvertently caching sensitive information. This issue was addressed with improved heuristics.

CVE-2017-7140: an anonymous researcher

Entry added September 25, 2017

libc

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A remote attacker may be able to cause a denial-of-service

Description: A resource exhaustion issue in glob() was addressed through an improved algorithm.

CVE-2017-7086: Russ Cox of Google

Entry added September 25, 2017

libc

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to cause a denial of service

Description: A memory consumption issue was addressed through improved memory handling.

CVE-2017-1000373

Entry added September 25, 2017

libexpat

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Multiple issues in expat

Description: Multiple issues were addressed by updating to version 2.2.1

CVE-2016-9063

CVE-2017-9233

Entry added September 25, 2017

Location Framework

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to read sensitive location information

Description: A permissions issue existed in the handling of the location variable. This was addressed with additional ownership checks.

CVE-2017-7148: an anonymous researcher, an anonymous researcher

Entry added September 25, 2017

Mail Drafts

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker with a privileged network position may be able to intercept mail contents

Description: An encryption issue existed in the handling of mail drafts. This issue was addressed with improved handling of mail drafts meant to be sent encrypted.

CVE-2017-7078: an anonymous researcher, an anonymous researcher, an anonymous researcher

Entry added September 25, 2017

Mail MessageUI

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing a maliciously crafted image may lead to a denial of service

Description: A memory corruption issue was addressed with improved validation.

CVE-2017-7097: Xinshu Dong and Jun Hao Tan of Anquan Capital

Messages

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing a maliciously crafted image may lead to a denial of service

Description: A denial of service issue was addressed through improved validation.

CVE-2017-7118: Kiki Jiang and Jason Tokoph

MobileBackup

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Backup may perform an unencrypted backup despite a requirement to perform only encrypted backups

Description: A permissions issue existed. This issue was addressed with improved permission validation.

CVE-2017-7133: Don Sparks of HackediOS.com

Phone

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A screenshot of secure content may be taken when locking an iOS device

Description: A timing issue existed in the handling of locking. This issue was addressed by disabling screenshots while locking.

CVE-2017-7139: an anonymous researcher

Entry added September 25, 2017

Safari

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Visiting a malicious website may lead to address bar spoofing

Description: An inconsistent user interface issue was addressed with improved state management.

CVE-2017-7085: xisigr of Tencent's Xuanwu Lab (tencent.com)

Security

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A revoked certificate may be trusted

Description: A certificate validation issue existed in the handling of revocation data. This issue was addressed through improved validation.

CVE-2017-7080: an anonymous researcher, an anonymous researcher, Sven Driemecker of adesso mobile solutions gmbh, Rune Darrud (@theflyingcorpse) of Bærum kommune

Entry added September 25, 2017

Security

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A malicious app may be able to track users between installs

Description: A permission checking issue existed in the handling of an app's Keychain data. This issue was addressed with improved permission checking.

CVE-2017-7146: an anonymous researcher

Entry added September 25, 2017

SQLite

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Multiple issues in SQLite

Description: Multiple issues were addressed by updating to version 3.19.3.

CVE-2017-10989: found by OSS-Fuzz

CVE-2017-7128: found by OSS-Fuzz

CVE-2017-7129: found by OSS-Fuzz

CVE-2017-7130: found by OSS-Fuzz

Entry added September 25, 2017

SQLite

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to execute arbitrary code with system privileges

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2017-7127: an anonymous researcher

Entry added September 25, 2017

Time

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: "Setting Time Zone" may incorrectly indicate that it is using location

Description: A permissions issue existed in the process that handles time zone information. The issue was resolved by modifying permissions.

CVE-2017-7145: an anonymous researcher

Entry added September 25, 2017

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

Description: A memory corruption issue was addressed through improved input validation.

CVE-2017-7081: Apple

Entry added September 25, 2017

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

Description: Multiple memory corruption issues were addressed with improved memory handling.

CVE-2017-7087: Apple

CVE-2017-7091: Wei Yuan of Baidu Security Lab working with Trend Micro’s Zero Day Initiative

CVE-2017-7092: Samuel Gro and Niklas Baumstark working with Trend Micro's Zero Day Initiative, Qixun Zhao (@S0rryMybad) of Qihoo 360 Vulcan Team

CVE-2017-7093: Samuel Gro and Niklas Baumstark working with Trend Micro’s Zero Day Initiative

CVE-2017-7094: Tim Michaud (@TimGMichaud) of Leviathan Security Group

CVE-2017-7095: Wang Junjie, Wei Lei, and Liu Yang of Nanyang Technological University working with Trend Micro’s Zero Day Initiative

CVE-2017-7096: Wei Yuan of Baidu Security Lab

CVE-2017-7098: Felipe Freitas of Instituto Tecnológico de Aeronáutica

CVE-2017-7099: Apple

CVE-2017-7100: Masato Kinugawa and Mario Heiderich of Cure53

CVE-2017-7102: Wang Junjie, Wei Lei, and Liu Yang of Nanyang Technological University

CVE-2017-7104: likemeng of Baidu Secutity Lab

CVE-2017-7107: Wang Junjie, Wei Lei, and Liu Yang of Nanyang Technological University

CVE-2017-7111: likemeng of Baidu Security Lab (xlab.baidu.com) working with Trend Micro's Zero Day Initiative

CVE-2017-7117: lokihardt of Google Project Zero

CVE-2017-7120: chenqin (陈钦) of Ant-financial Light-Year Security Lab

Entry added September 25, 2017

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing maliciously crafted web content may lead to universal cross site scripting

Description: A logic issue existed in the handling of the parent-tab. This issue was addressed with improved state management.

CVE-2017-7089: Anton Lopanitsyn of ONSEC, Frans Rosén of Detectify

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Cookies belonging to one origin may be sent to another origin

Description: A permissions issue existed in the handling of web browser cookies. This issue was addressed by no longer returning cookies for custom URL schemes.

CVE-2017-7090: Apple

Entry added September 25, 2017

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Visiting a malicious website may lead to address bar spoofing

Description: An inconsistent user interface issue was addressed with improved state management.

CVE-2017-7106: Oliver Paukstadt of Thinking Objects GmbH (to.com)

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Processing maliciously crafted web content may lead to a cross site scripting attack

Description: Application Cache policy may be unexpectedly applied.

CVE-2017-7109: avlidienbrunn

Entry added September 25, 2017

WebKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A malicious website may be able to track users in Safari private browsing mode

Description: A permissions issue existed in the handling of web browser cookies. This issue was addressed with improved restrictions.

CVE-2017-7144: an anonymous researcher

Entry added September 25, 2017

Wi-Fi

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker within range may be able to execute arbitrary code on the Wi-Fi chip

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2017-11120: Gal Beniamini of Google Project Zero

CVE-2017-11121: Gal Beniamini of Google Project Zero

Entry added September 25, 2017

Wi-Fi

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Malicious code executing on the Wi-Fi chip may be able to execute arbitrary code with kernel privileges on the application processor

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2017-7103: Gal Beniamini of Google Project Zero

CVE-2017-7105: Gal Beniamini of Google Project Zero

CVE-2017-7108: Gal Beniamini of Google Project Zero

CVE-2017-7110: Gal Beniamini of Google Project Zero

CVE-2017-7112: Gal Beniamini of Google Project Zero

Wi-Fi

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Malicious code executing on the Wi-Fi chip may be able to execute arbitrary code with kernel privileges on the application processor

Description: Multiple race conditions were addressed through improved validation.

CVE-2017-7115: Gal Beniamini of Google Project Zero

Wi-Fi

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Malicious code executing on the Wi-Fi chip may be able to read restricted kernel memory

Description: A validation issue was addressed with improved input sanitization.

CVE-2017-7116: Gal Beniamini of Google Project Zero

Wi-Fi

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A attacker within range may be able to read restricted memory from the Wi-Fi chipset

Description: A validation issue was addressed with improved input sanitization.

CVE-2017-11122: Gal Beniamini of Google Project Zero

Entry added October 2, 2017

zlib

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: Multiple issues in zlib

Description: Multiple issues were addressed by updating to version 1.2.11.

CVE-2016-9840

CVE-2016-9841

CVE-2016-9842

CVE-2016-9843

Entry added September 25, 2017

Additional recognition

Security

We would like to acknowledge Abhinav Bansal of Zscaler, Inc. for their assistance.

Webkit

We would like to acknowledge xisigr of Tencent's Xuanwu Lab (tencent.com) for their assistance.

Published Date: Oct 2, 2017

Helpful? Yes No

80% of people found this helpful.

Start a Discussion in Apple Support Communities

Ask other users about this article

Submit my question to the community

See all questions on this article › See all questions I have asked ›

Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.

Get started ›