About the security content of iOS 10.3

This document describes the security content of iOS 10.3.

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 10.3

Released March 27, 2017

Accounts

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A user may be able to view an Apple ID from the lock screen

Description: A prompt management issue was addressed by removing iCloud authentication prompts from the lock screen.

CVE-2017-2397: Suprovici Vadim of UniApps team, an anonymous researcher

Audio

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted audio file may lead to arbitrary code execution

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

CVE-2017-2430: an anonymous researcher working with Trend Micro's Zero Day Initiative

CVE-2017-2462: an anonymous researcher working with Trend Micro's Zero Day Initiative

Carbon

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted .dfont file may lead to arbitrary code execution

Description: A buffer overflow existed in the handling of font files. This issue was addressed through improved bounds checking.

CVE-2017-2379: John Villamil, Doyensec, riusksk (泉哥) of Tencent Security Platform Department

CoreGraphics

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: An infinite recursion was addressed through improved state management.

CVE-2017-2417: riusksk (泉哥) of Tencent Security Platform Department

CoreGraphics

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2444: Mei Wang of 360 GearTeam

CoreText

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted font file may lead to arbitrary code execution

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

CVE-2017-2435: John Villamil, Doyensec

CoreText

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: An out-of-bounds read was addressed through improved input validation.

CVE-2017-2450: John Villamil, Doyensec

CoreText

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted text message may lead to application denial of service

Description: A resource exhaustion issue was addressed through improved input validation.

CVE-2017-2461: Isaac Archambault of IDAoADI, an anonymous researcher

DataAccess

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Configuring an Exchange account with a mistyped email address may resolve to an unexpected server

Description: An input validation issue existed in the handling of Exchange email addresses. This issue was addressed through improved input validation.

CVE-2017-2414: Ilya Nesterov and Maxim Goncharov

FontParser

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted font file may lead to arbitrary code execution

Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2487: riusksk (泉哥) of Tencent Security Platform Department

CVE-2017-2406: riusksk (泉哥) of Tencent Security Platform Department

FontParser

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Parsing a maliciously crafted font file may lead to an unexpected application termination or arbitrary code execution

Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2407: riusksk (泉哥) of Tencent Security Platform Department

FontParser

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: An out-of-bounds read was addressed through improved input validation.

CVE-2017-2439: John Villamil, Doyensec

HomeKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Home Control may unexpectedly appear on Control Center

Description: A state issue existed in the handling of Home Control. This issue was addressed through improved validation.

CVE-2017-2434: Suyash Narain of India

HTTPProtocol

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A malicious HTTP/2 server may be able to cause undefined behavior

Description: Multiple issues existed in nghttp2 before 1.17.0. These were addressed by updating nghttp2 to version 1.17.0.

CVE-2017-2428

Entry updated March 28, 2017

ImageIO

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted image may lead to arbitrary code execution

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

CVE-2017-2416: Qidan He (何淇丹, @flanker_hqd) of KeenLab, Tencent

ImageIO

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Viewing a maliciously crafted JPEG file may lead to arbitrary code execution

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

CVE-2017-2432: an anonymous researcher working with Trend Micro's Zero Day Initiative

ImageIO

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted file may lead to an unexpected application termination or arbitrary code execution

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

CVE-2017-2467

ImageIO

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted image may lead to unexpected application termination

Description: An out-of-bound read existed in LibTIFF versions before 4.0.7. This was addressed by updating LibTIFF in ImageIO to version 4.0.7.

CVE-2016-3619

iTunes Store

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: An attacker in a privileged network position may be able to tamper with iTunes network traffic

Description: Requests to iTunes sandbox web services were sent in cleartext. This was addressed by enabling HTTPS.

CVE-2017-2412: Richard Shupak (linkedin.com/in/rshupak)

JavaScriptCore

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A use after free issue was addressed through improved memory management.

CVE-2017-2491: Apple

Entry added May 2, 2017

JavaScriptCore

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A prototype issue was addressed through improved logic.

CVE-2017-2492: lokihardt of Google Project Zero

Entry updated April 24, 2017

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2398: Lufeng Li of Qihoo 360 Vulcan Team

CVE-2017-2401: Lufeng Li of Qihoo 360 Vulcan Team

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: An integer overflow was addressed through improved input validation.

CVE-2017-2440: an anonymous researcher

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A malicious application may be able to execute arbitrary code with root privileges

Description: A race condition was addressed through improved memory handling.

CVE-2017-2456: lokihardt of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A use after free issue was addressed through improved memory management.

CVE-2017-2472: Ian Beer of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2473: Ian Beer of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: An off-by-one issue was addressed through improved bounds checking.

CVE-2017-2474: Ian Beer of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A race condition was addressed through improved locking.

CVE-2017-2478: Ian Beer of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A buffer overflow issue was addressed through improved memory handling.

CVE-2017-2482: Ian Beer of Google Project Zero

CVE-2017-2483: Ian Beer of Google Project Zero

Kernel

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2490: Ian Beer of Google Project Zero, The UK's National Cyber Security Centre (NCSC)

Entry added March 31, 2017

Keyboards

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: An application may be able to execute arbitrary code

Description: A buffer overflow was addressed through improved bounds checking.

CVE-2017-2458: Shashank (@cyberboyIndia)

Keychain

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: An attacker who is able to intercept TLS connections may be able to read secrets protected by iCloud Keychain.

Description: In certain circumstances, iCloud Keychain failed to validate the authenticity of OTR packets. This issue was addressed through improved validation.

CVE-2017-2448: Alex Radocea of Longterm Security, Inc.

Entry updated March 30, 2017

libarchive

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A local attacker may be able to change file system permissions on arbitrary directories

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

CVE-2017-2390: Omer Medan of enSilo Ltd

libc++abi

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Demangling a malicious C++ application may lead to arbitrary code execution

Description: A use after free issue was addressed through improved memory management.

CVE-2017-2441

libxslt

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Multiple vulnerabilities in libxslt

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

CVE-2017-5029: Holger Fuhrmannek

Entry added March 28, 2017

Pasteboard

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A person with physical access to an iOS device may read the pasteboard

Description: The pasteboard was encrypted with a key protected only by the hardware UID. This issue was addressed by encrypting the pasteboard with a key protected by the hardware UID and the user's passcode.

CVE-2017-2399

Phone

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A third party app can initiate a phone call without user interaction

Description: An issue existed in iOS allowing for calls without prompting. This issue was addressed by prompting a user to confirm call initiation.

CVE-2017-2484

Profiles

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: An attacker may be able to exploit weaknesses in the DES cryptographic algorithm

Description: Support for the 3DES cryptographic algorithm was added to the SCEP client and DES was deprecated.

CVE-2017-2380: an anonymous researcher

Quick Look

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Tapping a tel link in a PDF document could trigger a call without prompting the user

Description: An issue existed when checking the tel URL before initiating calls. This issue was addressed with the addition of a confirmation prompt.

CVE-2017-2404: Tuan Anh Ngo (Melbourne, Australia), Christoph Nehring

Safari

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A state management issue was addressed by disabling text input until the destination page loads.

CVE-2017-2376: an anonymous researcher, Michal Zalewski of Google Inc, Muneaki Nishimura (nishimunea) of Recruit Technologies Co., Ltd., Chris Hlady of Google Inc, an anonymous researcher, Yuyang Zhou of Tencent Security Platform Department (security.tencent.com)

Safari

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A local user may be able to discover websites a user has visited in Private Browsing

Description: An issue existed in SQLite deletion. This issue was addressed through improved SQLite cleanup.

CVE-2017-2384

Safari

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may present authentication sheets over arbitrary web sites

Description: A spoofing and denial-of-service issue existed in the handling of HTTP authentication. This issue was addressed through making HTTP authentication sheets non-modal.

CVE-2017-2389: ShenYeYinJiu of Tencent Security Response Center, TSRC

Safari

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Visiting a malicious website by clicking a link may lead to user interface spoofing

Description: A spoofing issue existed in the handling of FaceTime prompts. This issue was addressed through improved input validation.

CVE-2017-2453: xisigr of Tencent's Xuanwu Lab (tencent.com)

Safari Reader

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting

Description: Multiple validation issues were addressed through improved input sanitization.

CVE-2017-2393: Erling Ellingsen

SafariViewController

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Cache state is not properly kept in sync between Safari and SafariViewController when a user clears Safari cache

Description: An issue existed in clearing Safari cache information from SafariViewController. This issue was addressed by improving cache state handling.

CVE-2017-2400: Abhinav Bansal of Zscaler, Inc.

Sandbox Profiles

Available for: iPhone 5 and later, iPad 4th generation and later, and iPod touch 6th generation

Impact: A malicious application may be able to access the iCloud user record of a signed in user

Description: An access issue was addressed through additional sandbox restrictions on third party applications.

CVE-2017-6976: George Dan (@theninjaprawn)

Entry added August 1, 2017

Security

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Validating empty signatures with SecKeyRawVerify() may unexpectedly succeed

Description: An validation issue existed with cryptographic API calls. This issue was addressed through improved parameter validation.

CVE-2017-2423: an anonymous researcher

Security

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A buffer overflow was addressed through improved bounds checking.

CVE-2017-2451: Alex Radocea of Longterm Security, Inc.

Security

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing a maliciously crafted x509 certificate may lead to arbitrary code execution

Description: A memory corruption issue existed in the parsing of certificates. This issue was addressed through improved input validation.

CVE-2017-2485: Aleksandar Nikolic of Cisco Talos

Siri

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Siri might reveal text message contents while the device is locked

Description: An insufficient locking issue was addressed with improved state management.

CVE-2017-2452: Hunter Byrnes

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Dragging and dropping a maliciously crafted link may lead to bookmark spoofing or arbitrary code execution

Description: A validation issue existed in bookmark creation. This issue was addressed through improved input validation.

CVE-2017-2378: xisigr of Tencent's Xuanwu Lab (tencent.com)

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2486: redrain of light4freedom

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: A prototype access issue was addressed through improved exception handling.

CVE-2017-2386: André Bargull

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: Multiple memory corruption issues were addressed through improved input validation.

CVE-2017-2394: Apple

CVE-2017-2396: Apple

CVE-2016-9642: Gustavo Grieco

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2395: Apple

CVE-2017-2454: Ivan Fratric of Google Project Zero, Zheng Huang of the Baidu Security Lab working with Trend Micro's Zero Day Initiative

CVE-2017-2455: Ivan Fratric of Google Project Zero

CVE-2017-2457: lokihardt of Google Project Zero

CVE-2017-2459: Ivan Fratric of Google Project Zero

CVE-2017-2460: Ivan Fratric of Google Project Zero

CVE-2017-2464: Jeonghoon Shin, natashenka of Google Project Zero

CVE-2017-2465: Zheng Huang and Wei Yuan of Baidu Security Lab

CVE-2017-2466: Ivan Fratric of Google Project Zero

CVE-2017-2468: lokihardt of Google Project Zero

CVE-2017-2469: lokihardt of Google Project Zero

CVE-2017-2470: lokihardt of Google Project Zero

CVE-2017-2476: Ivan Fratric of Google Project Zero

CVE-2017-2481: 0011 working with Trend Micro's Zero Day Initiative

Entry updated June 20, 2017

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A type confusion issue was addressed through improved memory handling.

CVE-2017-2415: Kai Kang of Tencent's Xuanwu Lab (tentcent.com)

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may lead to unexpectedly unenforced Content Security Policy

Description: An access issue existed in Content Security Policy. This issue was addressed through improved access restrictions.

CVE-2017-2419: Nicolai Grødum of Cisco Systems

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may lead to high memory consumption

Description: An uncontrolled resource consumption issue was addressed through improved regex processing.

CVE-2016-9643: Gustavo Grieco

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may result in the disclosure of process memory

Description: An information disclosure issue existed in the processing of OpenGL shaders. This issue was addressed through improved memory management.

CVE-2017-2424: Paul Thomson (using the GLFuzz tool) of the Multicore Programming Group, Imperial College London

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2433: Apple

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: Multiple validation issues existed in the handling of page loading. This issue was addressed through improved logic.

CVE-2017-2364: lokihardt of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: A malicious website may exfiltrate data cross-origin

Description: A validation issue existed in the handling of page loading. This issue was addressed through improved logic.

CVE-2017-2367: lokihardt of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A logic issue existed in the handling of frame objects. This issue was addressed with improved state management.

CVE-2017-2445: lokihardt of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A logic issue existed in the handling of strict mode functions. This issue was addressed with improved state management.

CVE-2017-2446: natashenka of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Visiting a maliciously crafted website may compromise user information

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

CVE-2017-2447: natashenka of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2463: Kai Kang (4B5F5F4B) of Tencent's Xuanwu Lab (tencent.com) working with Trend Micro's Zero Day Initiative

Entry added March 28, 2017

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A use after free issue was addressed through improved memory management.

CVE-2017-2471: Ivan Fratric of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

Description: A logic issue existed in frame handling. This issue was addressed through improved state management.

CVE-2017-2475: lokihardt of Google Project Zero

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: A validation issue existed in element handling. This issue was addressed through improved validation.

CVE-2017-2479: lokihardt of Google Project Zero

Entry added March 28, 2017

WebKit

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: A validation issue existed in element handling. This issue was addressed through improved validation.

CVE-2017-2480: lokihardt of Google Project Zero

CVE-2017-2493: lokihardt of Google Project Zero

Entry updated April 24, 2017

WebKit JavaScript Bindings

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Processing maliciously crafted web content may exfiltrate data cross-origin

Description: Multiple validation issues existed in the handling of page loading. This issue was addressed through improved logic.

CVE-2017-2442: lokihardt of Google Project Zero

WebKit Web Inspector

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

Impact: Closing a window while paused in the debugger may lead to unexpected application termination

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

CVE-2017-2377: Vicki Pfau

WebKit Web Inspector

Available for: iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later

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

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

CVE-2017-2405: Apple

Additional recognition

XNU

We would like to acknowledge Lufeng Li of Qihoo 360 Vulcan Team for their assistance.

WebKit

We would like to acknowledge Yosuke HASEGAWA of Secure Sky Technology Inc. for their assistance.

Safari

We would like to acknowledge Flyin9 (ZhenHui Lee) for their assistance.

Settings

We would like to acknowledge Adi Sharabani and Yair Amit of Skycure for their assistance.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Contact the vendor for additional information.

Published Date: November 03, 2023

Helpful? Yes No

Support About the security content of iOS 10.3

Copyright © 2026 Apple Inc. All rights reserved. Privacy Policy | Terms of Use | Sales and Refunds | Site Map United States