About the security content of Safari 10.1

This document describes the security content of Safari 10.1.

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.

Safari 10.1

Released March 27, 2017

CoreGraphics

> Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

JavaScriptCore

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

Safari

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

Safari

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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 Login AutoFill

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

Impact: A local user may be able to access locked keychain items

Description: A keychain handling issue was addressed through improved keychain item management.

CVE-2017-2385: Simon Woodside of MedStack

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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-2017-2459: Ivan Fratric of Google Project Zero

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

CVE-2017-2464: Jeonghoon Shin, Natalie Silvanovich 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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: Natalie Silvanovich of Google Project Zero

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

Impact: Visiting a maliciously crafted website may compromise user information

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

CVE-2017-2447: Natalie Silvanovich of Google Project Zero

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: an anonymous researcher

Entry added March 30, 2017

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

Impact: An application may be able to execute arbitrary code

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

CVE-2017-2392: Max Bazaliy of Lookout

Entry added March 30, 2017

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

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

CVE-2017-2457: lokihardt of Google Project Zero

Entry added March 30, 2017

WebKit

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

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

CVE-2017-7071: Kai Kang (4B5F5F4B) of Tencent's Xuanwu Lab (tencent.com) working with Trend Micro's Zero Day Initiative

Entry added August 23, 2017

WebKit JavaScript Bindings

Available for: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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: OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12.4

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

Safari

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

Webkit

We would like to acknowledge Yosuke HASEGAWA of Secure Sky Technology Inc. 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: August 29, 2017

Helpful? Yes No

Contact Apple Support

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

Get started ›