About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan

This document describes the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan.

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.

macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan

Released October 31, 2017

apache

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Multiple issues in Apache

Description: Multiple issues were addressed by updating to version 2.4.27.

CVE-2016-0736

CVE-2016-2161

CVE-2016-5387

CVE-2016-8740

CVE-2016-8743

CVE-2017-3167

CVE-2017-3169

CVE-2017-7659

CVE-2017-7668

CVE-2017-7679

CVE-2017-9788

CVE-2017-9789

Entry updated November 14, 2017

APFS

Available for: macOS High Sierra 10.13

Impact: A malicious Thunderbolt adapter may be able to recover unencrypted APFS filesystem data

Description: An issue existed in the handling of DMA. This issue was addressed by limiting the time the FileVault decryption buffers are DMA mapped to the duration of the I/O operation.

CVE-2017-13786: Dmytro Oleksiuk

Entry updated November 10, 2017

APFS

Available for: macOS High Sierra 10.13

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-2017-13800: Sergej Schumilo of Ruhr-University Bochum

AppleScript

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Decompiling an AppleScript with osadecompile may lead to arbitrary code execution

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

CVE-2017-13809: bat0s

Entry updated November 10, 2017

ATS

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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

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

CVE-2017-13820: John Villamil, Doyensec

Audio

Available for: macOS Sierra 10.12.6

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

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

CVE-2017-13807: Yangkang (@dnpushme) of Qihoo 360 Qex Team

Entry updated January 22, 2019

CFNetwork

Available for: OS X El Capitan 10.11.6, and macOS Sierra 10.12.6

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-2017-13829: Niklas Baumstark and Samuel Gro working with Trend Micro's Zero Day Initiative

CVE-2017-13833: Niklas Baumstark and Samuel Gro working with Trend Micro's Zero Day Initiative

Entry added November 10, 2017

CFString

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An application may be able to read restricted memory

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

CVE-2017-13821: Australian Cyber Security Centre – Australian Signals Directorate

CoreText

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

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

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

CVE-2017-13825: Australian Cyber Security Centre – Australian Signals Directorate

Entry updated November 16, 2018

curl

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Uploading using TFTP to a maliciously crafted URL with libcurl may disclose application memory

Description: An out-of-bounds read was addressed with improved bounds checking.

CVE-2017-1000100: Even Rouault, found by OSS-Fuzz

curl

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Processing a maliciously crafted URL with libcurl may cause unexpected application termination or read process memory

Description: An out-of-bounds read was addressed with improved bounds checking.

CVE-2017-1000101: Brian Carpenter, Yongji Ouyang

Dictionary Widget

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Searching pasted text in the Dictionary widget may lead to compromise of user information

Description: A validation issue existed which allowed local file access. This was addressed with input sanitization.

CVE-2017-13801: xisigr of Tencent's Xuanwu Lab (tencent.com)

file

Available for: macOS Sierra 10.12.6

Impact: Multiple issues in file

Description: Multiple issues were addressed by updating to version 5.31.

CVE-2017-13815: found by OSS-Fuzz

Entry updated October 18, 2018

Fonts

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Rendering untrusted text may lead to spoofing

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

CVE-2017-13828: Leonard Grey and Robert Sesek of Google Chrome

Entry updated November 10, 2017

fsck_msdos

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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-2017-13811: V.E.O. (@VYSEa) of Mobile Advanced Threat Team of Trend Micro

Entry updated November 2, 2017

HFS

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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-2017-13830: Sergej Schumilo of Ruhr-University Bochum

Heimdal

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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 with improved validation.

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

Entry updated January 22, 2019

HelpViewer

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: A quarantined HTML file may execute arbitrary JavaScript cross-origin

Description: A cross-site scripting issue existed in HelpViewer. This issue was addressed by removing the affected file.

CVE-2017-13819: Filippo Cavallarin of SecuriTeam Secure Disclosure

Entry updated November 10, 2017

ImageIO

Available for: macOS Sierra 10.12.6

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

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

CVE-2017-13814: Australian Cyber Security Centre – Australian Signals Directorate

Entry updated November 16, 2018

ImageIO

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

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

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

CVE-2017-13831: Glen Carmichael

Entry updated April 3, 2019

IOAcceleratorFamily

Available for: macOS Sierra 10.12.6

Impact: A malicious application may be able to elevate privileges

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

CVE-2017-13906

Entry added October 18, 2018

Kernel

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: A local user may be able to leak sensitive user information

Description: A permissions issue existed in kernel packet counters. This issue was addressed with improved permission validation.

CVE-2017-13810: Zhiyun Qian of University of California, Riverside

Entry updated January 22, 2019

Kernel

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: A local user may be able to read kernel memory

Description: An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation.

CVE-2017-13817: Maxime Villard (m00nbsd)

Kernel

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An application may be able to read restricted memory

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

CVE-2017-13818: The UK's National Cyber Security Centre (NCSC)

CVE-2017-13836: Vlad Tsyrklevich

CVE-2017-13841: Vlad Tsyrklevich

CVE-2017-13840: Vlad Tsyrklevich

CVE-2017-13842: Vlad Tsyrklevich

CVE-2017-13782: Kevin Backhouse of Semmle Ltd.

Entry updated June 18, 2018

Kernel

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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-2017-13843: an anonymous researcher, an anonymous researcher

Kernel

Available for: macOS Sierra 10.12.6

Impact: Processing a malformed mach binary may lead to arbitrary code execution

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

CVE-2017-13834: Maxime Villard (m00nbsd)

Entry updated January 22, 2019

Kernel

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6

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-2017-13799: Lufeng Li of Qihoo 360 Vulcan Team

Entry updated November 10, 2017

Kernel

Available for: macOS High Sierra 10.13

Impact: A malicious application may be able to learn information about the presence and operation of other applications on the device.

Description: An application was able to access process information maintained by the operating system unrestricted. This issue was addressed with rate limiting.

CVE-2017-13852: Xiaokuan Zhang and Yinqian Zhang of The Ohio State University, Xueqiang Wang and XiaoFeng Wang of Indiana University Bloomington, and Xiaolong Bai of Tsinghua University

Entry added November 10, 2017, updated January 22, 2019

libarchive

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

Impact: Unpacking a maliciously crafted archive may lead to arbitrary code execution

Description: Multiple memory corruption issues existed in libarchive. These issues were addressed with improved input validation.

CVE-2017-13813: found by OSS-Fuzz

Entry updated November 16, 2018, updated January 22, 2019

libarchive

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Unpacking a maliciously crafted archive may lead to arbitrary code execution

Description: Multiple memory corruption issues existed in libarchive. These issues were addressed with improved input validation.

CVE-2017-13812: found by OSS-Fuzz

Entry updated January 22, 2019

libarchive

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An application may be able to read restricted memory

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

CVE-2016-4736: Proteas of Qihoo 360 Nirvan Team

Entry updated December 21, 2017

libxml2

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

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

Description: A null pointer dereference was addressed with improved validation.

CVE-2017-5969: Gustavo Grieco

Entry added October 18, 2018

libxml2

Available for: OS X El Capitan 10.11.6

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

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

CVE-2017-5130: an anonymous researcher

CVE-2017-7376: an anonymous researcher

Entry added October 18, 2018

libxml2

Available for: macOS Sierra 10.12.6

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

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

CVE-2017-9050: Mateusz Jurczyk (j00ru) of Google Project Zero

Entry added October 18, 2018

libxml2

Available for: macOS Sierra 10.12.6

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

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

CVE-2017-9049: Wei Lei and Liu Yang - Nanyang Technological University in Singapore

Entry added October 18, 2018

LinkPresentation

Available for: macOS High Sierra 10.13

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

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

CVE-2018-4390: Rayyan Bijoora (@Bijoora) of The City School, PAF Chapter

CVE-2018-4391: Rayyan Bijoora (@Bijoora) of The City School, PAF Chapter

Entry added November 16, 2018

Login Window

Available for: macOS High Sierra 10.13

Impact: The screen lock may unexpectedly remain unlocked

Description: A state management issue was addressed with improved state validation.

CVE-2017-13907: an anonymous researcher

Entry added October 18, 2018

Open Scripting Architecture

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Decompiling an AppleScript with osadecompile may lead to arbitrary code execution

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

CVE-2017-13824: an anonymous researcher

PCRE

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Multiple issues in pcre

Description: Multiple issues were addressed by updating to version 8.40.

CVE-2017-13846

Postfix

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: Multiple issues in Postfix

Description: Multiple issues were addressed by updating to version 3.2.2.

CVE-2017-10140: an anonymous researcher

Entry updated November 17, 2017

Quick Look

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An application may be able to read restricted memory

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

CVE-2017-13822: Australian Cyber Security Centre – Australian Signals Directorate

Quick Look

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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

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

CVE-2017-7132: Australian Cyber Security Centre – Australian Signals Directorate

Entry updated January 22, 2019

QuickTime

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An application may be able to read restricted memory

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

CVE-2017-13823: Xiangkun Jia of Institute of Software Chinese Academy of Sciences

Entry updated November 10, 2017

Remote Management

Available for: macOS Sierra 10.12.6

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-2017-13808: an anonymous researcher

Sandbox

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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-2017-13838: Alastair Houghton

Entry updated November 10, 2017

Security

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

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

Description: An authorization issue was addressed with improved state management.

CVE-2017-7170: Patrick Wardle of Synack

Entry added January 11, 2018

Security

Available for: macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: A malicious application can extract keychain passwords

Description: A method existed for applications to bypass the keychain access prompt with a synthetic click. This was addressed by requiring the user password when prompting for keychain access.

CVE-2017-7150: Patrick Wardle of Synack

Entry added November 17, 2017

SMB

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

Impact: A local attacker may be able to execute non-executable text files via an SMB share

Description: An issue in handling file permissions was addressed with improved validation.

CVE-2017-13908: an anonymous researcher

Entry added October 18, 2018

StreamingZip

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: A malicious zip file may be able modify restricted areas of the file system

Description: A path handling issue was addressed with improved validation.

CVE-2017-13804: @qwertyoruiopz at KJC Research Intl. S.R.L.

tcpdump

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6

Impact: Multiple issues in tcpdump

Description: Multiple issues were addressed by updating to version 4.9.2.

CVE-2017-11108

CVE-2017-11541

CVE-2017-11542

CVE-2017-11543

CVE-2017-12893

CVE-2017-12894

CVE-2017-12895

CVE-2017-12896

CVE-2017-12897

CVE-2017-12898

CVE-2017-12899

CVE-2017-12900

CVE-2017-12901

CVE-2017-12902

CVE-2017-12985

CVE-2017-12986

CVE-2017-12987

CVE-2017-12988

CVE-2017-12989

CVE-2017-12990

CVE-2017-12991

CVE-2017-12992

CVE-2017-12993

CVE-2017-12994

CVE-2017-12995

CVE-2017-12996

CVE-2017-12997

CVE-2017-12998

CVE-2017-12999

CVE-2017-13000

CVE-2017-13001

CVE-2017-13002

CVE-2017-13003

CVE-2017-13004

CVE-2017-13005

CVE-2017-13006

CVE-2017-13007

CVE-2017-13008

CVE-2017-13009

CVE-2017-13010

CVE-2017-13011

CVE-2017-13012

CVE-2017-13013

CVE-2017-13014

CVE-2017-13015

CVE-2017-13016

CVE-2017-13017

CVE-2017-13018

CVE-2017-13019

CVE-2017-13020

CVE-2017-13021

CVE-2017-13022

CVE-2017-13023

CVE-2017-13024

CVE-2017-13025

CVE-2017-13026

CVE-2017-13027

CVE-2017-13028

CVE-2017-13029

CVE-2017-13030

CVE-2017-13031

CVE-2017-13032

CVE-2017-13033

CVE-2017-13034

CVE-2017-13035

CVE-2017-13036

CVE-2017-13037

CVE-2017-13038

CVE-2017-13039

CVE-2017-13040

CVE-2017-13041

CVE-2017-13042

CVE-2017-13043

CVE-2017-13044

CVE-2017-13045

CVE-2017-13046

CVE-2017-13047

CVE-2017-13048

CVE-2017-13049

CVE-2017-13050

CVE-2017-13051

CVE-2017-13052

CVE-2017-13053

CVE-2017-13054

CVE-2017-13055

CVE-2017-13687

CVE-2017-13688

CVE-2017-13689

CVE-2017-13690

CVE-2017-13725

Wi-Fi

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An attacker in Wi-Fi range may force nonce reuse in WPA unicast/PTK clients (Key Reinstallation Attacks - KRACK)

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

CVE-2017-13077: Mathy Vanhoef of the imec-DistriNet group at KU Leuven

CVE-2017-13078: Mathy Vanhoef of the imec-DistriNet group at KU Leuven

Entry updated November 3, 2017

Wi-Fi

Available for: macOS High Sierra 10.13, macOS Sierra 10.12.6, OS X El Capitan 10.11.6

Impact: An attacker in Wi-Fi range may force nonce reuse in WPA multicast/GTK clients (Key Reinstallation Attacks - KRACK)

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

CVE-2017-13080: Mathy Vanhoef of the imec-DistriNet group at KU Leuven

Entry updated November 3, 2017

Published Date: November 03, 2023