About the security content of macOS Big Sur 11.3

This document describes the security content of macOS Big Sur 11.3.

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.

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

For more information about security, see the Apple Product Security page.

macOS Big Sur 11.3

Released April 26, 2021

APFS

Available for: macOS Big Sur

Impact: A local attacker may be able to elevate their privileges

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

CVE-2021-1853: Gary Nield of ECSC Group plc and Tim Michaud(@TimGMichaud) of Zoom Video Communications

AppleMobileFileIntegrity

Available for: macOS Big Sur

Impact: A malicious application may be able to bypass Privacy preferences

Description: An issue in code signature validation was addressed with improved checks.

CVE-2021-1849: Siguza

Apple Neural Engine

Available for: macOS Big Sur

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

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

CVE-2021-1867: Zuozhi Fan (@pattern_F_) and Wish Wu(吴潍浠) of Ant Group Tianqiong Security Lab

Archive Utility

Available for: macOS Big Sur

Impact: A malicious application may bypass Gatekeeper checks

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

CVE-2021-1810: Rasmus Sten (@pajp) of F-Secure

Entry updated on April 27, 2021

Audio

Available for: macOS Big Sur

Impact: An application may be able to read restricted memory

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

CVE-2021-1808: JunDong Xie of Ant Security Light-Year Lab

CFNetwork

Available for: macOS Big Sur

Impact: Processing maliciously crafted web content may disclose sensitive user information

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

CVE-2021-1857: an anonymous researcher

Compression

Available for: macOS Big Sur

Impact: An out-of-bounds read was addressed with improved input validation

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

CVE-2021-30752: Ye Zhang (@co0py_Cat) of Baidu Security

Entry added July 21, 2021

CoreAudio

Available for: macOS Big Sur

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

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

CVE-2021-30664: JunDong Xie of Ant Security Light-Year Lab

Entry added May 6, 2021

CoreAudio

Available for: macOS Big Sur

Impact: Processing a maliciously crafted audio file may disclose restricted memory

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

CVE-2021-1846: JunDong Xie of Ant Security Light-Year Lab

CoreAudio

Available for: macOS Big Sur

Impact: A malicious application may be able to read restricted memory

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

CVE-2021-1809: JunDong Xie of Ant Security Light-Year Lab

CoreFoundation

Available for: macOS Big Sur

Impact: A malicious application may be able to leak sensitive user information

Description: A validation issue was addressed with improved logic.

CVE-2021-30659: Thijs Alkemade of Computest

CoreGraphics

Available for: macOS Big Sur

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

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

CVE-2021-1847: Xuwei Liu of Purdue University

CoreText

Available for: macOS Big Sur

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

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

CVE-2021-1811: Xingwei Lin of Ant Security Light-Year Lab

curl

Available for: macOS Big Sur

Impact: A malicious server may be able to disclose active services

Description: This issue was addressed with improved checks.

CVE-2020-8284: Marian Rehak

Entry added May 6, 2021

curl

Available for: macOS Big Sur

Impact: An attacker may provide a fraudulent OCSP response that would appear valid

Description: This issue was addressed with improved checks.

CVE-2020-8286: an anonymous researcher

curl

Available for: macOS Big Sur

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

Description: A buffer overflow was addressed with improved input validation.

CVE-2020-8285: xnynx

DiskArbitration

Available for: macOS Big Sur

Impact: A malicious application may be able to modify protected parts of the file system

Description: A permissions issue existed in DiskArbitration. This was addressed with additional ownership checks.

CVE-2021-1784: Mikko Kenttälä (@Turmio_) of SensorFu, Csaba Fitzl (@theevilbit) of Offensive Security, and an anonymous researcher

FaceTime

Available for: macOS Big Sur

Impact: Muting a CallKit call while ringing may not result in mute being enabled

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

CVE-2021-1872: Siraj Zaneer of Facebook

FontParser

Available for: macOS Big Sur

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

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

CVE-2021-1881: an anonymous researcher, Xingwei Lin of Ant Security Light-Year Lab, Mickey Jin of Trend Micro, and Hou JingYi (@hjy79425575) of Qihoo 360

Foundation

Available for: macOS Big Sur

Impact: An application may be able to gain elevated privileges

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

CVE-2021-1882: Gabe Kirkpatrick (@gabe_k)

Foundation

Available for: macOS Big Sur

Impact: A malicious application may be able to gain root privileges

Description: A validation issue was addressed with improved logic.

CVE-2021-1813: Cees Elzinga

Heimdal

Available for: macOS Big Sur

Impact: Processing maliciously crafted server messages may lead to heap corruption

Description: This issue was addressed with improved checks.

CVE-2021-1883: Gabe Kirkpatrick (@gabe_k)

Heimdal

Available for: macOS Big Sur

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

Description: A race condition was addressed with improved locking.

CVE-2021-1884: Gabe Kirkpatrick (@gabe_k)

ImageIO

Available for: macOS Big Sur

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

Description: This issue was addressed with improved checks.

CVE-2021-1880: Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-30653: Ye Zhang of Baidu Security

CVE-2021-1814: Ye Zhang of Baidu Security, Mickey Jin & Qi Sun of Trend Micro, and Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-1843: Ye Zhang of Baidu Security

ImageIO

Available for: macOS Big Sur

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

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

CVE-2021-1885: CFF of Topsec Alpha Team

ImageIO

Available for: macOS Big Sur

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

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

CVE-2021-1858: Mickey Jin of Trend Micro

ImageIO

Available for: macOS Big Sur

Impact: An out-of-bounds write was addressed with improved input validation

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

CVE-2021-30743: Ye Zhang (@co0py_Cat) of Baidu Security, CFF of Topsec Alpha Team, Jzhu working with Trend Micro Zero Day Initiative, Xingwei Lin of Ant Security Light-Year Lab, CFF of Topsec Alpha Team, Jeonghoon Shin (@singi21a) of THEORI working with Trend Micro Zero Day Initiative

Entry added July 21, 2021

Installer

Available for: macOS Big Sur

Impact: A malicious application may bypass Gatekeeper checks

Description: This issue was addressed with improved handling of file metadata.

CVE-2021-30658: Wojciech Reguła (@_r3ggi) of SecuRing

Intel Graphics Driver

Available for: macOS Big Sur

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

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

CVE-2021-1841: Jack Dates of RET2 Systems, Inc.

CVE-2021-1834: ABC Research s.r.o. working with Trend Micro Zero Day Initiative

Kernel

Available for: macOS Big Sur

Impact: A malicious application may be able to disclose kernel memory

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

CVE-2021-1860: @0xalsr

Kernel

Available for: macOS Big Sur

Impact: A local attacker may be able to elevate their privileges

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

CVE-2021-1840: Zuozhi Fan (@pattern_F_) of Ant Group Tianqiong Security Lab

Kernel

Available for: macOS Big Sur

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

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

CVE-2021-1851: @0xalsr

Kernel

Available for: macOS Big Sur

Impact: Copied files may not have the expected file permissions

Description: The issue was addressed with improved permissions logic.

CVE-2021-1832: an anonymous researcher

Kernel

Available for: macOS Big Sur

Impact: A malicious application may be able to disclose kernel memory

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

CVE-2021-30660: Alex Plaskett

libxpc

Available for: macOS Big Sur

Impact: A malicious application may be able to gain root privileges

Description: A race condition was addressed with additional validation.

CVE-2021-30652: James Hutchins

libxslt

Available for: macOS Big Sur

Impact: Processing a maliciously crafted file may lead to heap corruption

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

CVE-2021-1875: Found by OSS-Fuzz

Login Window

Available for: macOS Big Sur

Impact: A malicious application with root privileges may be able to access private information

Description: This issue was addressed with improved entitlements.

CVE-2021-1824: Wojciech Reguła (@_r3ggi) of SecuRing

Notes

Available for: macOS Big Sur

Impact: Locked Notes content may have been unexpectedly unlocked

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

CVE-2021-1859: Syed Ali Shuja (@SyedAliShuja) of Colour King Pvt. Ltd

NSRemoteView

Available for: macOS Big Sur

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

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

CVE-2021-1876: Matthew Denton of Google Chrome

Preferences

Available for: macOS Big Sur

Impact: A local user may be able to modify protected parts of the file system

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2021-1815: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

CVE-2021-1739: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

CVE-2021-1740: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

Safari

Available for: macOS Big Sur

Impact: A malicious website may be able to track users by setting state in a cache

Description: An issue existed in determining cache occupancy. The issue was addressed through improved logic.

CVE-2021-1861: Konstantinos Solomos of University of Illinois at Chicago

Safari

Available for: macOS Big Sur

Impact: A malicious website may be able to force unnecessary network connections to fetch its favicon

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

CVE-2021-1855: Håvard Mikkelsen Ottestad of HASMAC AS

SampleAnalysis

Available for: macOS Big Sur

Impact: A local attacker may be able to elevate their privileges

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

CVE-2021-1868: Tim Michaud of Zoom Communications

Sandbox

Available for: macOS Big Sur

Impact: A malicious application may be able to access the user's recent contacts

Description: The issue was addressed with improved permissions logic.

CVE-2021-30750: Csaba Fitzl (@theevilbit) of Offensive Security

Entry added May 28, 2021

smbx

Available for: macOS Big Sur

Impact: An attacker in a privileged network position may be able to leak sensitive user information

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

CVE-2021-1878: Aleksandar Nikolic of Cisco Talos (talosintelligence.com)

System Preferences

Available for: macOS Big Sur

Impact: A malicious application may bypass Gatekeeper checks. Apple is aware of a report that this issue may have been actively exploited.

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

CVE-2021-30657: Cedric Owens (@cedowens)

Entry added April 27, 2021, updated April 30, 2021

TCC

Available for: macOS Big Sur

Impact: A malicious unsandboxed app on a system with Remote Login enabled may bypass Privacy preferences

Description: This issue was addressed by adding a new Remote Login option for opting into Full Disk Access for Secure Shell sessions.

CVE-2021-30856: Csaba Fitzl (@theevilbit) of Offensive Security, Andy Grant of Zoom Video Communications, Thijs Alkemade of Computest Research Division, Wojciech Reguła of SecuRing (wojciechregula.blog), Cody Thomas of SpecterOps, Mickey Jin of Trend Micro

Entry added January 19, 2022, updated May 25, 2022

tcpdump

Available for: macOS Big Sur

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

Description: This issue was addressed with improved checks.

CVE-2020-8037: an anonymous researcher

Time Machine

Available for: macOS Big Sur

Impact: A local attacker may be able to elevate their privileges

Description: The issue was addressed with improved permissions logic.

CVE-2021-1839: Tim Michaud(@TimGMichaud) of Zoom Video Communications and Gary Nield of ECSC Group plc

WebKit

Available for: macOS Big Sur

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

Description: An input validation issue was addressed with improved input validation.

CVE-2021-1825: Alex Camboe of Aon's Cyber Solutions

WebKit

Available for: macOS Big Sur

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

Description: A memory corruption issue was addressed with improved state management.

CVE-2021-1817: zhunki

Entry updated May 6, 2021

WebKit

Available for: macOS Big Sur

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

Description: A logic issue was addressed with improved restrictions.

CVE-2021-1826: an anonymous researcher

WebKit

Available for: macOS Big Sur

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

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

CVE-2021-1820: André Bargull

Entry updated May 6, 2021

WebKit Storage

Available for: macOS Big Sur

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

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

CVE-2021-30661: yangkang(@dnpushme) of 360 ATA

WebRTC

Available for: macOS Big Sur

Impact: A remote attacker may be able to cause unexpected system termination or corrupt kernel memory

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

CVE-2020-7463: Megan2013678

Wi-Fi

Available for: macOS Big Sur

Impact: An application may be able to cause unexpected system termination or write kernel memory

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

CVE-2021-1828: Zuozhi Fan (@pattern_F_) of Ant Group Tianqiong Security Lab

Wi-Fi

Available for: macOS Big Sur

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

Description: A type confusion issue was addressed with improved state handling.

CVE-2021-1829: Tielei Wang of Pangu Lab

Wi-Fi

Available for: macOS Big Sur

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

Description: The issue was addressed with improved permissions logic.

CVE-2021-30655: Gary Nield of ECSC Group plc and Tim Michaud(@TimGMichaud) of Zoom Video Communications and Wojciech Reguła (@_r3ggi) of SecuRing

Wi-Fi

Available for: macOS Big Sur

Impact: A logic issue was addressed with improved state management

Description: A buffer overflow may result in arbitrary code execution.

CVE-2021-1770: Jiska Classen (@naehrdine) of Secure Mobile Networking Lab, TU Darmstadt

Entry added July 21, 2021

WindowServer

Available for: macOS Big Sur

Impact: A malicious application may be able to unexpectedly leak a user's credentials from secure text fields

Description: An API issue in Accessibility TCC permissions was addressed with improved state management.

CVE-2021-1873: an anonymous researcher

Additional recognition

AirDrop

We would like to acknowledge @maxzks for their assistance.

Entry added May 6, 2021

CoreAudio

We would like to acknowledge an anonymous researcher for their assistance.

Entry added May 6, 2021

CoreCrypto

We would like to acknowledge Andy Russon of Orange Group for their assistance.

Entry added May 6, 2021

File Bookmark

We would like to acknowledge an anonymous researcher for their assistance.

Entry added May 6, 2021

Foundation

We would like to acknowledge CodeColorist of Ant-Financial LightYear Labs for their assistance.

Entry added May 6, 2021

Kernel

We would like to acknowledge Antonio Frighetto of Politecnico di Milano, GRIMM, Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan, Mikko Kenttälä (@Turmio_) of SensorFu, and Proteas for their assistance.

Entry added May 6, 2021

Mail

We would like to acknowledge Petter Flink, SecOps of Bonnier News and an anonymous researcher for their assistance.

Entry added May 6, 2021

Safari

We would like to acknowledge Sahil Mehra (Nullr3x) & Shivam Kamboj Dattana (Sechunt3r) for their assistance.

Entry added May 6, 2021

Security

We would like to acknowledge Xingwei Lin of Ant Security Light-Year Lab and john (@nyan_satan) for their assistance.

Entry added May 6, 2021

sysdiagnose

We would like to acknowledge Tim Michaud (@TimGMichaud) of Leviathan for their assistance.

Entry added May 6, 2021

WebKit

We would like to acknowledge Emilio Cobos Álvarez of Mozilla for their assistance.

Entry added May 6, 2021

WebSheet

We would like to acknowledge Patrick Clover for their assistance.

Entry added May 6, 2021

Published Date: November 02, 2023