You are invited to take part in a short survey to help us improve your Apple Support online experience. Please select Yes if you would like to participate.

Yes No

About the security content of macOS Big Sur 11.6

This document describes the security content of macOS Big Sur 11.6.

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 11.6

Released September 13, 2021

AppleMobileFileIntegrity

Available for: macOS Big Sur

Impact: A local attacker may be able to read sensitive information

Description: This issue was addressed with improved checks.

CVE-2021-30811: an anonymous researcher working with Compartir

Entry added January 19, 2022

Apple Neural Engine

Available for: macOS Big Sur

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

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

CVE-2021-30838: proteas wang

Entry added January 19, 2022

CoreAudio

Available for: macOS Big Sur

Impact: Processing a malicious audio file may result in unexpected application termination or arbitrary code execution

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

CVE-2021-30834: JunDong Xie of Ant Security Light-Year Lab

Entry added January 19, 2022

CoreGraphics

Available for: macOS Big Sur

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

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

CVE-2021-30928: Mickey Jin (@patch1t) of Trend Micro

Entry added January 19, 2022

CoreGraphics

Available for: macOS Big Sur

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

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

CVE-2021-30860: The Citizen Lab

Core Telephony

Available for: macOS Big Sur

Impact: A sandboxed process may be able to circumvent sandbox restrictions. Apple was aware of a report that this issue may have been actively exploited at the time of release.

Description: A deserialization issue was addressed through improved validation.

CVE-2021-31010: Citizen Lab and Google Project Zero

Entry added May 25, 2022

CUPS

Available for: macOS Big Sur

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

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

CVE-2021-30827: an anonymous researcher

Entry added September 20, 2021

CUPS

Available for: macOS Big Sur

Impact: A local user may be able to read arbitrary files as root

Description: This issue was addressed with improved checks.

CVE-2021-30828: an anonymous researcher

Entry added September 20, 2021

CUPS

Available for: macOS Big Sur

Impact: A local user may be able to execute arbitrary files

Description: A URI parsing issue was addressed with improved parsing.

CVE-2021-30829: an anonymous researcher

Entry added September 20, 2021

curl

Available for: macOS Big Sur

Impact: curl could potentially reveal sensitive internal information to the server using a clear-text network protocol

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

CVE-2021-22925: Red Hat Product Security

Entry added September 20, 2021, updated January 19, 2022

CVMS

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 state management.

CVE-2021-30832: Mickey Jin (@patch1t) of Trend Micro

Entry added September 20, 2021

FontParser

Available for: macOS Big Sur

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

Description: This issue was addressed with improved checks.

CVE-2021-30841: Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-30842: Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-30843: Xingwei Lin of Ant Security Light-Year Lab

Entry added September 20, 2021

Gatekeeper

Available for: macOS Big Sur

Impact: A malicious application may bypass Gatekeeper checks

Description: This issue was addressed with improved checks.

CVE-2021-30853: Gordon Long (@ethicalhax) of Box, Inc.

Entry added September 20, 2021

Graphics Drivers

Available for: macOS Big Sur

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

Description: A race condition was addressed with improved state handling.

CVE-2021-30933: Jack Dates of RET2 Systems, Inc.

Entry added May 25, 2022

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-2021-30835: Ye Zhang of Baidu Security

Entry added January 19, 2022

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-2021-30847: Mike Zhang of Pangu Lab

Entry added September 20, 2021

Kernel

Available for: macOS Big Sur

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

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

CVE-2021-30830: Zweig of Kunlun Lab

Entry added September 20, 2021

Kernel

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-2021-30865: Zweig of Kunlun Lab

Entry added September 20, 2021

Kernel

Available for: macOS Big Sur

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

Description: A race condition was addressed with improved locking.

CVE-2021-30857: Zweig of Kunlun Lab

Entry added September 20, 2021

Kernel

Available for: macOS Big Sur

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

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

CVE-2021-30859: Apple

Entry added September 20, 2021

LaunchServices

Available for: macOS Big Sur

Impact: A sandboxed process may be able to circumvent sandbox restrictions

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

CVE-2021-30864: Ron Hass (@ronhass7) of Perception Point, Ron Waisberg (@epsilan)

Entry added January 19, 2022

libexpat

Available for: macOS Big Sur

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

Description: This issue was addressed by updating expat to version 2.4.1.

CVE-2013-0340: an anonymous researcher

Entry added September 20, 2021

Login Window

Available for: macOS Big Sur

Impact: A person with access to a host Mac may be able to bypass the Login Window in Remote Desktop for a locked instance of macOS

Description: A logic issue was addressed with improved checks.

CVE-2021-30813: Benjamin Berger of BBetterTech LLC, Aaron Hines of AHDesigns916, Peter Goedtkindt of Informatique-MTF S.A.

Entry added May 25, 2022

Model I/O

Available for: macOS Big Sur

Impact: Processing a maliciously crafted USD file may disclose memory contents

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

CVE-2021-30819

Entry added January 19, 2022

Preferences

Available for: macOS Big Sur

Impact: An application may be able to access restricted files

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

CVE-2021-30855: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

Entry added September 20, 2021

Sandbox

Available for: macOS Big Sur

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

Description: The issue was addressed with improved permissions logic.

CVE-2021-30925: Csaba Fitzl (@theevilbit) of Offensive Security

Entry added January 19, 2022

Sandbox

Available for: macOS Big Sur

Impact: A user may gain access to protected parts of the file system

Description: An access issue was addressed with improved access restrictions.

CVE-2021-30850: an anonymous researcher

Entry added September 20, 2021

SMB

Available for: macOS Big Sur

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

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

CVE-2021-30845: Peter Nguyen Vu Hoang of STAR Labs

Entry added September 20, 2021

SMB

Available for: macOS Big Sur

Impact: A remote attacker may be able to leak memory

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

CVE-2021-30844: Peter Nguyen Vu Hoang of STAR Labs

Entry added September 20, 2021

WebKit

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-2021-30858: an anonymous researcher

Additional recognition

APFS

We would like to acknowledge Koh M. Nakagawa of FFRI Security, Inc., for their assistance.

Entry added September 20, 2021, updated June 21, 2022

App Support

We would like to acknowledge @CodeColorist, an anonymous researcher, and 漂亮鼠 of 赛博回忆录 for their assistance.

Entry added September 20, 2021, updated May 25, 2022

CoreML

We would like to acknowledge hjy79425575 working with Trend Micro Zero Day Initiative for their assistance.

Entry added September 20, 2021

CUPS

We would like to acknowledge an anonymous researcher, Inc., and Nathan Nye of WhiteBeam Security for their assistance.

Entry added September 20, 2021, updated May 25, 2022

Kernel

We would like to acknowledge Anthony Steinhauser of Google's Safeside project for their assistance.

Entry added September 20, 2021

Sandbox

We would like to acknowledge Csaba Fitzl (@theevilbit) of Offensive Security for their assistance.

Entry added September 20, 2021

smbx

We would like to acknowledge Zhongcheng Li (CK01) for their assistance.

Entry added September 20, 2021

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 02, 2023

Helpful? Yes No

Support > About the security content of macOS Big Sur 11.6

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