



Site Search

[Full Disclosure](#) mailing list archives[← By Date →](#) [← By Thread →](#)

List Archive Search



APPLE-SA-2021-09-20-7 Additional information for APPLE-SA-2021-09-13-3 macOS Big Sur 11.6

From: product-security-noreply--- via Fulldisclosure <fulldisclosure () seclists org>
Date: Mon, 20 Sep 2021 14:44:31 -0700

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

APPLE-SA-2021-09-20-7 Additional information for
APPLE-SA-2021-09-13-3 macOS Big Sur 11.6

macOS Big Sur 11.6 addresses the following issues.
Information about the security content is also available at
<https://support.apple.com/HT212804>.

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

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

Entry added September 20, 2021

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

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

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

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 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

App Support

We would like to acknowledge @CodeColorist, an anonymous researcher for their assistance.
Entry added September 20, 2021

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 for their assistance.
Entry added September 20, 2021

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

Installation note:

This update may be obtained from the Mac App Store or Apple's Software Downloads web site:
<https://support.apple.com/downloads/>

Information will also be posted to the Apple Security Updates web site: <https://support.apple.com/kb/HT201222>

This message is signed with Apple's Product Security PGP key, and details are available at:
<https://www.apple.com/support/security/pgp/>

-----BEGIN PGP SIGNATURE-----

```
iQIzBAEBCAAAdFiEEePiLW1MrMjw19XzoeC9qKD1prhgFamFI888ACgkQeC9qKD1p
rhi/Bg/9GiqXl8sxPjDpATJqneZ1GcAxWxBZgkFrclV/cMwrVqniWs0eVHqHjMSY
eJUKGehUtKsYE0g8Uk0qJq0Ul3dxxGJpIDyt0QJB3TFdd1BpZSK/t0ChVem1JV1B
+CMhqDnmR/u7bLqfCr1p6J5QJNHjtjgBA4RthdzZZ52pLGql7/2qfaJwpeHkheS4
5EKmch8zh0CGRqrUTg1HgY67ierNsz47jIU6n7UeMwjskRU3xM9VqJ9s4eKGAAtSv
4Ry16pv0xUZ4cmL5EiLm2/eFbY8ByCji7jYPP0P0B04l518TGpaX2PaZBP9v0rrD
t6cPEZHnsRaZ490Yak6z9iA8teKGSs6aCMuzSxExvlT8+YySf1o1nefbRH/tZMfn
bwS00ZyPsS9WYyuG/zX08U3CK0TkjqhLa0wVwte+cAeg2QS85aa9XPMG6PKcypyfu
R7auxS92+Dg+R+97dAsI9TprSutCTw4iY8lyK9MVJSnh+zQSZEihUh4EaSufTHRC
NlOSHvsTfXqsHaeed6sVKyX4ADHCuvRbCCIrqJKUs6waNd2T2XF7SsvgTSDJMHU9
4AL/jpnltTjDJTtM0999VZKNzYurrGiHvBs5zHWr91+eaHW8YGdsDERsX3BFYLe3
85i+Yge0iXlP7mT32cwXiw4AWDFITFiHnmV1/cdsCd2GIkqkhFw=
=9bjT
```

-----END PGP SIGNATURE-----

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[↩ By Date ↪](#) [↩ By Thread ↪](#)

Current thread:

APPLE-SA-2021-09-20-7 Additional information for APPLE-SA-2021-09-13-3 macOS Big Sur 11.6 product-security-noreply--- via Fulldisclosure (Sep 21)

Site Search



Nmap Security Scanner

- Ref Guide
- Install Guide
- Docs
- Download
- Nmap OEM

Npcap packet capture

- User's Guide
- API docs
- Download
- Npcap OEM

Security Lists

- Nmap Announce
- Nmap Dev
- Full Disclosure
- Open Source Security
- BreachExchange

Security Tools

- Vuln scanners
- Password audit
- Web scanners
- Wireless
- Exploitation

About

- About/Contact
- Privacy
- Advertising
- Nmap Public Source License

