Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Vulnerability Note CIVN-2022-0240
Multiple vulnerabilities in Apple macOS

Original Issue Date:May 19, 2022

Severity Rating: CRITICAL

Software Affected

- Apple macOS Catalina prior to security update 2022-004
- Apple macOS Big Sur versions prior to 11.6.6
- Apple macOS Monterey versions prior to 12.4

Overview

Multiple vulnerabilities have been reported in Apple macOS which could be exploited by a remote attacker to execute arbitrary code, bypass security restrictions and cause denial of service conditions on the targeted system.

Description

Multiple vulnerabilities exist in Apple macOS due to use after free in Kernel & libxml2; memory corruption in AppleGraphicsControl, Intel Graphics Driver, Kernel, Wi-Fi, zlib, IOMobileFrameBuffer & SMB; memory initialization in CVMS; race condition in IOKit; integer overflow in libresolv & ImageIO;out-of-bounds read errors in AppleScript, Intel Graphics Driver & SMB; out-of-bounds write errors in Intel Graphics Driver, SMB, AppleAVD & AVEVideoEncoder; logic issue in AppKit & ImageIO;denial of service in LibreSSL & zip; memory initialization issue in CVMS; improper validation in symlinks and certificate parsing issue in Security component. A remote attacker could exploit these vulnerabilities a victim to visit a maliciously crafted webpage.

Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code, bypass security restrictions, integer overflow, gain root privileges, cause denial of service conditions on the targeted system.

Solution

Apply appropriate security updates as mentioned in the [Apple Security Update](#)

Vendor Information

Apple
https://support.apple.com/en-us/HT213255
https://support.apple.com/en-us/HT213256
https://support.apple.com/en-us/HT213257

References

Apple
https://support.apple.com/en-us/HT213255
https://support.apple.com/en-us/HT213256
https://support.apple.com/en-us/HT213257

CVE Name
CVE-2018-25032
CVE-2021-4136
CVE-2021-4166
CVE-2021-4173
CVE-2021-4187
CVE-2021-4192
CVE-2021-4193
CVE-2021-44224
CVE-2021-44790
CVE-2021-45444
CVE-2021-46059
CVE-2022-0128
CVE-2022-0530
CVE-2022-0778
CVE-2022-22589
CVE-2022-22663
CVE-2022-22665

[CVE-2022-22674](#)
[CVE-2022-22675](#)
[CVE-2022-22677](#)
[CVE-2022-22719](#)
[CVE-2022-22720](#)
[CVE-2022-22721](#)
[CVE-2022-23308](#)
[CVE-2022-26693](#)
[CVE-2022-26694](#)
[CVE-2022-26697](#)
[CVE-2022-26698](#)
[CVE-2022-26700](#)
[CVE-2022-26701](#)
[CVE-2022-26704](#)
[CVE-2022-26706](#)
[CVE-2022-26708](#)
[CVE-2022-26709](#)
[CVE-2022-26710](#)
[CVE-2022-26711](#)
[CVE-2022-26712](#)
[CVE-2022-26714](#)
[CVE-2022-26715](#)
[CVE-2022-26716](#)
[CVE-2022-26717](#)
[CVE-2022-26718](#)
[CVE-2022-26719](#)
[CVE-2022-26720](#)
[CVE-2022-26721](#)
[CVE-2022-26722](#)
[CVE-2022-26723](#)
[CVE-2022-26725](#)
[CVE-2022-26726](#)
[CVE-2022-26727](#)
[CVE-2022-26728](#)
[CVE-2022-26731](#)
[CVE-2022-26736](#)
[CVE-2022-26737](#)
[CVE-2022-26738](#)
[CVE-2022-26739](#)
[CVE-2022-26740](#)
[CVE-2022-26741](#)
[CVE-2022-26742](#)
[CVE-2022-26743](#)
[CVE-2022-26745](#)
[CVE-2022-26746](#)
[CVE-2022-26748](#)
[CVE-2022-26749](#)
[CVE-2022-26750](#)
[CVE-2022-26751](#)
[CVE-2022-26752](#)
[CVE-2022-26753](#)
[CVE-2022-26754](#)
[CVE-2022-26755](#)
[CVE-2022-26756](#)
[CVE-2022-26757](#)
[CVE-2022-26761](#)
[CVE-2022-26762](#)
[CVE-2022-26763](#)
[CVE-2022-26764](#)
[CVE-2022-26765](#)
[CVE-2022-26766](#)
[CVE-2022-26767](#)
[CVE-2022-26768](#)
[CVE-2022-26769](#)
[CVE-2022-26770](#)
[CVE-2022-26772](#)
[CVE-2022-26775](#)
[CVE-2022-26776](#)

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India