Severity

High

Analysis Summary

CVE-2022-26691 CVSS:7.8 Apple macOS Monterey and macOS Big Sur could allow a local authenticated attacker to gain elevated privileges on the system, caused by a logic issue in the CUPS component. By using a specially-crafted application, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

CVE-2022-26690 CVSS:6.2 Apple macOS Monterey could allow a local attacker to bypass security restrictions, caused by a race condition issue in the PackageKit component. By using a specially-crafted application, an attacker could exploit this vulnerability to modify protected parts of the file system.

CVE-2022-26688 CVSS:4.4 Apple macOS Monterey and macOS Big Sur could allow a local authenticated attacker to bypass security restrictions, caused by an issue in the handling of symlinks in the PackageKit component. By using a specially-crafted application, an attacker could exploit this vulnerability to modify the contents of system files.

CVE-2022-22676 CVSS:6.8 Apple macOS Monterey could allow a local attacker to bypass security restrictions, caused by an event handler validation issue in the XPC Services API in the PackageKit component. By using a specially-crafted application, an attacker could exploit this vulnerability to delete files on the system.

CVE-2022-22672 CVSS:8.4 Apple macOS Monterey, iOS and iPadOS could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption issue in the MobileAccessoryUpdater component. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code code with kernel privileges.

CVE-2021-31010 CVSS:8.4 Apple macOS Big Sur, watchOS, iOS and iPadOS could allow a local attacker to execute arbitrary code on the system, caused by a deserialization issue in the Core Telephony component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass sandbox restrictions to execute arbitrary code on the system.

CVE-2021-31009 CVSS:6.2 An unspecified error with multiple issues in HDF5 in Apple macOS Monterey, iOS and iPadOS has an unknown impact and attack vector.

CVE-2021-31008 CVSS:8.8 Apple Safari, tvOS, watchOS, macOS Monterey, iOS and iPadOS could allow a remote attacker to execute arbitrary code on the system, caused by a type confusion issue in the WebKit component. By persuading a victim to visit a specially-crafted web content, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2021-31007 CVSS:6.2 Apple macOS Big Sur, macOS Monterey, tvOS, watchOS, iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a permissions issue in the File Provider component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass Privacy preferences.

CVE-2021-31006 CVSS:6.2 Apple macOS Big Sur, watchOS, and tvOS could allow a local attacker to bypass security restrictions, caused by a permissions issue in the App Store component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass certain Privacy preferences.

CVE-2021-31005 CVSS:4 Apple macOS Monterey, iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a logic issue in the WebKit component. By using a specially-crafted application, an attacker could exploit this vulnerability to cause turning off “Block all remote content” not apply to all remote content types.

CVE-2021-31001 CVSS:6.5 Apple iOS and iPadOS could allow a remote attacker to obtain sensitive information, caused by an access issue in the Telephony component. By sending a specially-crafted request, an attacker could exploit this vulnerability to continue to obtain sensitive user information.

CVE-2021-31000 CVSS:4 Apple macOS Monterey, tvOS, watchOS, iOS and iPadOS could allow a local attacker to obtain sensitive information, caused by a permissions issue in the Game Center component. By using a specially-crafted application, an attacker could exploit this vulnerability to read sensitive contact information.

CVE-2021-30999 CVSS:4 Apple iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a permissions issue in the Safari component. By using a specially-crafted application, an attacker could exploit this vulnerability to fully delete the browsing history.

CVE-2021-30998 CVSS:4 Apple iOS and iPadOS could allow a local attacker to obtain sensitive information, caused by a S/MIME issue existed in the handling of encrypted email in the Mail component. By sending a specially-crafted request, an attacker could exploit this vulnerability to the sender's email address.

CVE-2021-30997 CVSS:6.2 Apple iOS and iPadOS could allow a local attacker to obtain sensitive information, caused by a S/MIME issue existed in the handling of encrypted email in the Mail component. By sending a specially-crafted request, an attacker could exploit this vulnerability to recover plaintext contents of an S/MIME-encrypted e-mail.

CVE-2021-30994 CVSS:4 Apple macOS Monterey could allow a local attacker to obtain sensitive information, caused by an access issue in the App Store component. By using a specially-crafted application, an attacker could exploit this vulnerability to disclose local users' Apple IDs.

CVE-2021-30962 CVSS:4 Apple macOS Big Sur and tvOS could allow a local attacker to obtain sensitive information, caused by a memory initialization issue in the CoreAudio component. By using a specially-crafted audio file, an attacker could exploit this vulnerability to disclose user information.

CVE-2021-30956 CVSS:2.4 Apple iOS and iPadOS could allow a physical attacker to obtain sensitive information, caused by a lock screen issue in the FaceTime component. By performing specially-crafted operations, an attacker could exploit this vulnerability to access to contacts on a locked device.

CVE-2021-30944 CVSS:4 Apple macOS Monterey, tvOS, watchOS, iOS and iPadOS could allow a local attacker to obtain sensitive information, caused by a logic issue in the SQLite component. By using a specially-crafted application, an attacker could exploit this vulnerability to access data from other apps by enabling additional logging.

CVE-2021-30943 CVSS:5.3 Apple macOS Monterey, watchOS, iOS and iPadOS could allow a remote attacker to obtain sensitive information, caused by an issue in the handling of group membership in the Messages component. By sending a specially-crafted request, an attacker could exploit this vulnerability to continue to receive messages after leaving a messages group.

CVE-2021-30933 CVSS: Apple macOS Monterey could allow a local authenticated attacker to execute arbitrary code on the system, caused by a race condition flaw in the Graphics Drivers component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

Impact

- Privilege Escalation
- Security Bypass
- Code Execution
- Gain Access
- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-26691
- CVE-2022-26690
- CVE-2022-26688
- CVE-2022-22676
- CVE-2022-22672
- CVE-2021-31010
- CVE-2021-31009
- CVE-2021-31008
- CVE-2021-31007
- CVE-2021-31006
- CVE-2021-31005
- CVE-2021-31001
- CVE-2021-31000
- CVE-2021-30999

- CVE-2021-30998
- CVE-2021-30997
- CVE-2021-30994
- CVE-2021-30962
- CVE-2021-30956
- CVE-2021-30944
- CVE-2021-30943
- CVE-2021-30933

Affected Vendors

- Apple

Affected Products

- Apple macOS Monterey 12.2.0
- Apple macOS Big Sur 11.6.4
- Apple macOS Monterey 12.1
- Apple iOS 15.3
- Apple iPadOS 15.3
- Apple macOS Big Sur 11.5.0
- Apple watchOS 7.6.1
- Apple iOS 14.7
- Apple iPadOS 14.7
- Apple iPadOS 14.8
- Apple iOS 14.8
- Apple tvOS 15.0
- Apple watchOS 8.0
- Apple watchOS 7.5.0
- Apple tvOS 14.6
- Apple macOS Big Sur 11.4.0
- Apple iOS 15.1
- Apple iPadOS 15.1

Remediation

Refer to Apple security Advisory for patch, upgrade or suggested workaround information.

Apple macOS Monterey 12.3

Apple macOS Monterey 12.2

Apple iOS 15.2 and iPadOS 15.2

Apple iOS 15 and iPadOS 15

Apple iOS 15.1 and iPadOS 15.1

Apple macOS Big Sur 11.5

Apple watchOS 8.3

Apple iPadOS 14.6 and iOS 14.6

Apple macOS Monterey 12.0.1

Apple macOS Big Sur 11.6.2