Severity

High

Analysis Summary

CVE-2022-26776 CVSS:7.8

Apple macOS Big Sur could allow a remote attacker to execute arbitrary code on the system, caused by a flaw in the libresolv component. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service.

CVE-2022-26767 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an issue in the LaunchServices component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass Privacy preferences.

CVE-2022-26770 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds read issue in the Intel Graphics Driver component. By executing a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26769 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue in the Intel Graphics Driver component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26761 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue in the Wi-Fi component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26756 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the Intel Graphics Driver component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26755 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an issue in the Tcl component. By using a specially-crafted application, an attacker could exploit this vulnerability to break out of its sandbox.

CVE-2022-26748 CVSS:7.8

Apple macOS Big Sur could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write issue in the Intel Graphics Driver component. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-26746 CVSS:7.8

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an issue in the Printing component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass Privacy preferences.

CVE-2022-26728 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an issue in the SoftwareUpdate component. By using a specially-crafted application, an attacker could exploit this vulnerability to access restricted files.

CVE-2022-26723 CVSS:9.8

Apple macOS Big Sur could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption issue in the SMB component. By mounting a maliciously crafted Samba network share, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-26722 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by a memory initialization issue in the CVMS component. By executing a specially-crafted application, an attacker could exploit this vulnerability to gain root privileges on the system.

CVE-2022-26720 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the Intel Graphics Driver component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26718 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds read issue in the SMB component. By executing a specially-crafted application, an attacker could exploit this vulnerability to gain elevated privileges on the system.

CVE-2022-26715 CVSS:8.4

Apple macOS Big Sur could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the SMB component. By executing a specially-crafted application, an attacker could exploit this vulnerability to gain elevated privileges on the system.

CVE-2022-26712 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an 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-2022-26698 CVSS:5.5

Apple macOS Big Sur is vulnerable to a denial of service, caused by an out-of-bounds read issue in the AppleScript component. By processing a specially crafted AppleScript binary, an attacker could exploit this vulnerability to cause a denial of service or obtain sensitive information.

CVE-2022-26697 CVSS:7.1

Apple macOS Big Sur is vulnerable to a denial of service, caused by an out-of-bounds read issue in the AppleScript component. By processing a specially crafted AppleScript binary, an attacker could exploit this vulnerability to cause a denial of service or obtain sensitive information.

CVE-2022-22663 CVSS:5.5

Apple macOS Big Sur could allow a local attacker to bypass security restrictions, caused by an issue in the CoreTypes component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass Gatekeeper checks.

CVE-2022-26693 CVSS:5.5

Apple macOS Monterey could allow a local attacker to obtain sensitive information, caused by a flaw in the Preview component. By executing a specially-crafted application, an attacker could exploit this vulnerability to inherit the application’s permissions and access user data.

CVE-2022-26694 CVSS:5.5

Apple macOS Monterey could allow a local attacker to obtain sensitive information, caused by a flaw in the Contacts component. By executing a specially-crafted application, an attacker could exploit this vulnerability to gain access to user data, and use this information to launch further attacks against the affected system.

CVE-2022-26704 CVSS:7.8

Apple macOS Monterey could allow a local attacker to gain elevated privileges on the system, caused by a improper handling of symlinks in the Spotlight component. By executing a specially-crafted application, an authenticated attacker could exploit this vulnerability to gain elevated privileges.

CVE-2022-26708 CVSS:7.8

Apple macOS Monterey could allow a local authenticated attacker to execute arbitrary code on the system, caused by a flaw in the libresolv component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code or cause unexpected application termination.

CVE-2022-26725 CVSS:6.2

Apple macOS Monterey could allow a local attacker to obtain sensitive information, caused by a flaw in the ImageIO component. By executing a specially crafted application, an attacker could exploit this vulnerability to obtain Photo location information, and use this information to launch further attacks against the affected system.

CVE-2022-26727 CVSS:6.2

Apple macOS Monterey could allow a local attacker to bypass security restrictions, caused by a flaw in the PackageKit component. By executing a specially-crafted application, an attacker could exploit this vulnerability to modify protected parts of the file system.

CVE-2022-26741 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26742 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26743 CVSS:7.8

Apple macOS Monterey could allow a local authenticated attacker to gain elevated privileges on the system, caused by an out-of-bounds write flaw in the Kernel component. By sending a specially-crafted request, an authenticated attacker could exploit this vulnerability to gain kernel privileges.

CVE-2022-26749 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26750 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26752 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26753 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26754 CVSS:7.8

Apple macOS Monterey is vulnerable to a buffer overflow, caused by improper bounds checking by the AMD component. By executing a specially-crafted application, a local authenticated attacker could overflow a buffer and execute arbitrary code with kernel privileges.

CVE-2022-26770 CVSS:7.8

Apple macOS Monterey could allow a local authenticated attacker to execute arbitrary code on the system, caused by an out-of-bounds read flaw in the Intel Graphics Driver. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26772 CVSS:7.8

Apple macOS Monterey could allow a local authenticated attacker to execute arbitrary code on the system, caused by a memory corruption flaw in the AMD component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26775 CVSS:7.8

Apple macOS Monterey could allow a local authenticated attacker to execute arbitrary code on the system, caused by an integer overflow in the libresolv component. By executing a specially-crafted application, an attacker could exploit this vulnerability to execute arbitrary code or cause unexpected application termination.

Impact

- Code Execution
- Privilege Escalation
- Denial of Service
- Buffer Overflow

Indicators Of Compromise

CVE

- CVE-2022-26776
- CVE-2022-26767
- CVE-2022-26770
- CVE-2022-26769
- CVE-2022-26761
- CVE-2022-26756
- CVE-2022-26755
- CVE-2022-26748
- CVE-2022-26746
- CVE-2022-26728
- CVE-2022-26723
- CVE-2022-26722
- CVE-2022-26720
- CVE-2022-26718
- CVE-2022-26715
- CVE-2022-26712
- CVE-2022-26698

- CVE-2022-26697
- CVE-2022-22663
- CVE-2022-26693
- CVE-2022-26694
- CVE-2022-26704
- CVE-2022-26708
- CVE-2022-26725
- CVE-2022-26727
- CVE-2022-26741
- CVE-2022-26742
- CVE-2022-26743
- CVE-2022-26749
- CVE-2022-26750
- CVE-2022-26752
- CVE-2022-26753
- CVE-2022-26754
- CVE-2022-26770
- CVE-2022-26772
- CVE-2022-26775

Affected Vendors

- Apple

Affected Products

- Apple macOS Big Sur 11.6.5
- Apple macOS Monterey 12.3

Remediation

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

Apple macOS Big Sur

Apple macOS Monterey