Severity

High

Analysis Summary

CVE-2022-26736 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the AVEVideoEncoder component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26737 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the AVEVideoEncoder component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26738 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the AVEVideoEncoder component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26739 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the AVEVideoEncoder component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26740 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds write issue in the AVEVideoEncoder component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26763 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by an out-of-bounds access issue in the DriverKit component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with system privileges.

CVE-2022-26744 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue in the GPU Drivers component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26711 CVSS:7.8

Apple iOS and iPadOS could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow in the ImageIO 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-2022-26701 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by a race condition in the IOKit component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26768 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue in the IOMobileFrameBuffer component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26714 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue in the Kernel component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26757 CVSS:7.8

Apple iOS and iPadOS could allow a local attacker to gain elevated privileges on the system, caused by a use-after-free in the Kernel component. By using a specially crafted application, an attacker could exploit this vulnerability to execute arbitrary code with kernel privileges.

CVE-2022-26765 CVSS:5.5

Apple iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a race condition in the Kernel component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass Pointer Authentication.

CVE-2022-26706 CVSS:5.5

Apple iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by an access issue in the LaunchServices component. By using a specially-crafted application, an attacker could exploit this vulnerability to circumvent sandbox restrictions.

CVE-2022-22673 CVSS:5.5

Apple iOS and iPadOS are vulnerable to a denial of service, caused by a flaw in the Notes component. By processing a large input, an attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-26731 CVSS:5.5

Apple iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a logic issue in the Safari Private Browsing component. By persuading a victim to visit a specially-crafted Web site, an attacker could exploit this vulnerability to track users in Safari private browsing mode.

CVE-2022-26766 CVSS:5.5

Apple iOS and iPadOS could allow a local attacker to bypass security restrictions, caused by a certificate parsing issue in the Security component. By using a specially-crafted application, an attacker could exploit this vulnerability to bypass signature validation.

Impact

- Privilege Escalation
- Security Bypass

Indicators Of Compromise

CVE

- CVE-2022-26736
- CVE-2022-26737
- CVE-2022-26738
- CVE-2022-26739
- CVE-2022-26740
- CVE-2022-26763
- CVE-2022-26744

- CVE-2022-26711
- CVE-2022-26701
- CVE-2022-26768
- CVE-2022-26714
- CVE-2022-26757
- CVE-2022-26765
- CVE-2022-26706
- CVE-2022-22673
- CVE-2022-26731
- CVE-2022-26766

Affected Vendors

- Apple iOS
- Apple iPadOS

Affected Products

- Apple iOS 15.4
- Apple iPadOS 15.4

Remediation

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

Apple security document