ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Apple iOS 15: iPhones — iOS 15.7.1

Maintenance Update of Apple iOS 15: iPhones — iOS 15.1.0

Maintenance Report Number: CCEVS-VR-VID11237-2022

Date of Activity: November 30, 2022

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;

Apple iOS 15: iPhones Impact Analysis Report for Common Criteria Assurance Maintenance v1.1, November 28, 2022

Certified TOE: **Apple iOS 15, Specific Version iOS 15.1.0, Validation Report Number: CCEVS-VR-VID11237-2022**

Maintained TOE: **Apple iOS 15, Specific Version iOS 15.1.7**

Documentation Updated:

The following table show how the original documentation has been updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Certified Security Target: Apple iOS 15: iPhones Security Target, Version 1.2, 2022-09-29.	**Maintained Security Target:** Apple iOS 15: iPhones Security Target, Version 1.3, 2022-11-09. Security Target is modified to change the TOE OS version from 15.1.0 to 15.7.1. No other change to content is made.

Assurance Continuity Maintenance Report

The atsec CCTL submitted the latest Impact Analysis Report (IAR) and Assurance Continuity Maintenance package on behalf of Apple Inc to the CCEVS for approval on November 23, 2022. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes

Changes to TOE:

The TOE version of iOS 15.1.0 is changed to iOS 15.7.1. The only changes were made to fix publicly disclosed vulnerabilities (CVEs). Assurance activities previously performed are not repeated and are still applicable.

There were no changes to the hardware or Development Environment.

The tables in Appendix A are summarized from the IAR. The tables provide brief explanation of the changes to fix the CVEs for several TOE versions leading to iOS 15.7.1.

All publicly disclosed security vulnerabilities applicable to all versions of the TOE prior to the Maintained TOE have been mitigated as illustrated in the tables in Appendix A. All fixes are considered minor in terms of functionality change as they merely correct unintended behavior.

The validation Team has reviewed the rationale for being minor and agree with the verdicts.

Recent Search for Known Vulnerabilities:

The search was repeated on October 27, 2022, upon the release of iOS 15.7.1 and again on November 28, 2022.

The evaluator searched the following databases for CVEs applicable to the product.

- MITRE Common Vulnerabilities and Exposures (CVE) List
- NIST National Vulnerability Database (NVD)
- Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Catalog

The search terms used in both the evaluation of VID11237 and for this assurance maintenance were the following.

- ios iphone
- ios core tls
- ios core crypto
- ios common crypto
- ios http
- ios https
- ios tcp

- ios ip
- ios bluetooth
- ios ipsec
- ios vpn
- ios mdm
- ios mobile
- ios touchid
- ios faceid
- broadcom wi-fi

The evaluator performed these searches and found no additional CVEs.

Cryptography:

No cryptographic functionality is modified in the maintained product, therefore all CAVP certificates obtained for VID11237 and listed in the AAR are still applicable.

Regression testing:

Regression testing of iOS for every release is performed by the vendor. All identified CVEs are managed through Apple Product Security where initial research and impact are identified through extensive analysis of the submission, scope and depth across all Apple products, versions, and source code. Once analysis is completed, remediation begins with development of an appropriate patch that is unit tested locally by lead engineers. Submissions are then tested by Security QA Testers and after all tests/checks are passed, the patch is submitted to mainline for broader OS regression testing. Upon full pass, the patch is staged and released for updating by users.

Based regression testing, Apple Inc. asserts the changed product still performs correctly and as expected after these changes.

Conclusion:

Based on vulnerability and regression testing described in the previous section, the vendor asserts that the changed product still conforms to the SF and SAR claims set forth in the initial evaluation. CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

Appendix A — List of Product Changes

The tables provide brief explanation of the changes to fix the CVEs for several TOE versions leading to iOS 15.7.1.

Table 1: Vulnerabilities fixed in iOS 15.2.0

Vulnerability ID	Component	Impact	Mitigation
CVE-2021-30960	Audio	Parsing a maliciously crafted audio file may lead to disclosure of user information.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30966	CFNetwork Proxies	User traffic might unexpectedly be leaked to a proxy server despite PAC configurations.	A logic issue was addressed with improved state management.
CVE-2021-30926	ColorSync	Processing a maliciously crafted image may lead to arbitrary code execution.	A memory corruption issue in the processing of ICC profiles was addressed with improved input validation.
CVE-2021-30942	ColorSync	Processing a maliciously crafted image may lead to arbitrary code execution.	A memory corruption issue in the processing of ICC profiles was addressed with improved input validation.
CVE-2021-30957	CoreAudio	Processing a maliciously crafted audio file may lead to arbitrary code execution.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30958	CoreAudio	Playing a malicious audio file may lead to arbitrary code execution.	An out-of-bounds read was addressed with improved input validation.
CVE-2021-30945	Crash Reporter	A local attacker may be able to elevate their privileges.	This issue was addressed with improved checks.
CVE-2021-30956	FaceTime	An attacker with physical access to a device may be able to see private contact information.	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management.
CVE-2021-30992	FaceTime	A user in a FaceTime call may unexpectedly leak sensitive user information through Live Photos metadata.	This issue was addressed with improved handling of file metadata.
CVE-2021-31000	Game Center	A malicious application may be able to read sensitive contact information.	A permissions issue was addressed with improved validation.
CVE-2021-30939	ImageIO	Processing a maliciously crafted image may lead to arbitrary code execution.	An out-of-bounds read was addressed with improved bounds checking.
CVE-2021-30996	IOMobile-FrameBuffer	A malicious application may be able to execute arbitrary code with kernel privileges.	A race condition was addressed with improved state handling.
CVE-2021-30983	IOMobile-FrameBuffer	An application may be able to execute arbitrary code with kernel privileges.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30985	IOMobile-FrameBuffer	A malicious application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2021-30991	IOMobile-FrameBuffer	A malicious application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds read was addressed with improved bounds checking.
CVE-2021-30937	Kernel	A malicious application may be able to execute arbitrary code with kernel privileges.	A memory corruption vulnerability was addressed with improved locking.
CVE-2021-30927	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.

CVE-2021-30980	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2021-30949	Kernel	A malicious application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved state management.
CVE-2021-30993	Kernel	An attacker in a privileged network position may be able to execute arbitrary code.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30955	Kernel	A malicious application may be able to execute arbitrary code with kernel privileges	A race condition was addressed with improved state handling.
CVE-2021-30998	Mail	A sender's email address may be leaked when sending an S/MIME encrypted email using a certificate with more than one email address.	A S/MIME issue existed in the handling of encrypted email. This issue was addressed with improved selection of the encryption certificate.
CVE-2021-30997	Mail	An attacker may be able to recover plaintext contents of an S/MIME-encrypted e-mail.	A S/MIME issue existed in the handling of encrypted email. This issue was addressed by not automatically loading some MIME parts.
CVE-2021-30943	Messages	A malicious user may be able to leave a messages group but continue to receive messages in that group.	An issue in the handling of group membership was resolved with improved logic.
CVE-2021-31009	Model I/O	Multiple issues in HDF5.	Multiple issues were addressed by removing HDF5.
CVE-2021-30971	Model I/O	Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2021-30973	Model I/O	Processing a maliciously crafted file may disclose user information.	An out-of-bounds read was addressed with improved input validation.
CVE-2021-30929	Model I/O	Processing a maliciously crafted USD file may disclose memory contents.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2021-30979	Model I/O	Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30940	Model I/O	Processing a maliciously crafted USD file may disclose memory contents.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30941	Model I/O	Processing a maliciously crafted USD file may disclose memory contents.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30967	Network-Extension	A local attacker may be able to read sensitive information.	A permissions issue was addressed with improved validation.
CVE-2021-30988	Network-Extension	A malicious application may be able to identify what other applications a user has installed.	A permissions issue was addressed with improved validation.
CVE-2021-30932	Notes	A person with physical access to an iOS device may be able to access contacts from the lock screen.	The issue was addressed with improved permissions logic.
CVE-2021-30948	Password Manager	A person with physical access to an iOS device may be able to access stored passwords without authentication.	An inconsistent user interface issue was addressed with improved state management.
CVE-2021-30995	Preferences	A malicious application may be able to elevate privileges.	A race condition was addressed with improved state handling.
CVE-2021-30968	Sandbox	A malicious application may be able to bypass certain Privacy preferences.	A validation issue related to hard link behavior was addressed with improved sandbox restrictions.
CVE-2021-30946	Sandbox	A malicious application may be able to bypass certain Privacy preferences.	A logic issue was addressed with improved restrictions.
CVE-2021-30947	Sandbox	An application may be able to access a user's files.	An access issue was addressed with additional sandbox restrictions.

CVE-2021-30944	SQLite	A malicious app may be able to access data from other apps by enabling additional logging.	A logic issue was addressed with improved state management.
CVE-2021-30767	TCC	A local user may be able to modify protected parts of the file system.	A logic issue was addressed with improved state management.
CVE-2021-30964	TCC	A malicious application may be able to bypass Privacy preferences.	An inherited permissions issue was addressed with additional restrictions.
CVE-2021-30934	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A buffer overflow issue was addressed with improved memory handling.
CVE-2021-30936	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2021-30951	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2021-30952	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	An integer overflow was addressed with improved input validation.
CVE-2021-30984	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A race condition was addressed with improved state handling.
CVE-2021-30953	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	An out-of-bounds read was addressed with improved bounds checking.
CVE-2021-30954	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A type confusion issue was addressed with improved memory handling.

Table 1: Vulnerabilities fixed in iOS 15.2.1

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-22588	HomeKit	Processing a maliciously crafted HomeKit accessory name may cause a denial of service.	A resource exhaustion issue was addressed with improved input validation.

Table 2: Vulnerabilities fixed in iOS 15.3

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-22584	ColorSync	Processing a maliciously crafted file may lead to arbitrary code execution.	A memory corruption issue was addressed with improved validation.
CVE-2022-22578	Crash Reporter	A malicious application may be able to gain root privileges.	A logic issue was addressed with improved validation.
CVE-2022-22585	iCloud	An application may be able to access a user's files.	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization.
CVE-2022-22587	IOMobileFrameBuffer	A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	A memory corruption issue was addressed with improved input validation.

CVE-2022-22593	Kernel	A malicious application may be able to execute arbitrary code with kernel privileges.	A buffer overflow issue was addressed with improved memory handling.
CVE-2022-22590	WebKit	Processing a maliciously crafted mail message may lead to running arbitrary javascript.	A validation issue was addressed with improved input sanitization.
CVE-2022-22592	WebKit	Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	A logic issue was addressed with improved state management.
CVE-2022-22594	WebKit Storage	A website may be able to track sensitive user information.	A cross-origin issue in the IndexDB API was addressed with improved input validation.

Table 3: Vulnerabilities fixed in iOS 15.3.1

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-22620	WebKit	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.	A use after free issue was addressed with improved memory management.

Table 4: Vulnerabilities fixed in iOS 15.4

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-22633	Accelerate Framework	Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	A memory corruption issue was addressed with improved state management.
CVE-2022-22666	AppleAVD	Processing a maliciously crafted image may lead to heap corruption.	A memory corruption issue was addressed with improved validation.
CVE-2022-22634	AVEVideoEncoder	A malicious application may be able to execute arbitrary code with kernel privileges.	A buffer overflow was addressed with improved bounds checking.
CVE-2022-22635	AVEVideoEncoder	An application may be able to gain elevated privileges	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-22636	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-22652	Cellular	A person with physical access may be able to view and modify the carrier account information and settings from the lock screen.	The GSMA authentication panel could be presented on the lock screen. The issue was resolved by requiring device unlock to interact with the GSMA authentication panel.
CVE-2022-22598	CoreMedia	An app may be able to learn information about the current camera view before being granted camera access.	An issue with app access to camera metadata was addressed with improved logic.
CVE-2022-22663	CoreTypes	A malicious application may bypass Gatekeeper checks.	This issue was addressed with improved checks to prevent unauthorized actions.
CVE-2022-22642	FaceTime	A user may be able to bypass the Emergency SOS passcode prompt.	This issue was addressed with improved checks.
CVE-2022-22643	FaceTime	A user may send audio and video in a FaceTime call without knowing that they have done so.	This issue was addressed with improved checks.

CVE-2022-22667	GPU Drivers	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-22611	ImageIO	Processing a maliciously crafted image may lead to arbitrary code execution.	An out-of-bounds read was addressed with improved input validation.
CVE-2022-22612	ImageIO	Processing a maliciously crafted image may lead to heap corruption.	A memory consumption issue was addressed with improved memory handling.
CVE-2022-22641	IOGPUFamily	An application may be able to gain elevated privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-22653	iTunes	A malicious website may be able to access information about the user and their devices.	A logic issue was addressed with improved restrictions.
CVE-2022-22596	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved validation.
CVE-2022-22640	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved validation.
CVE-2022-22613	Kernel	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-22614	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-22615	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-22632	Kernel	A malicious application may be able to elevate privileges.	A logic issue was addressed with improved state management.
CVE-2022-22638	Kernel	An attacker in a privileged position may be able to perform a denial of service attack.	A null pointer dereference was addressed with improved validation.
CVE-2021-36976	libarchive	Multiple issues in libarchive.	Multiple memory corruption issues existed in libarchive. These issues were addressed with improved input validation.
CVE-2022-21658	LLVM	An application may be able to delete files for which it does not have permission.	A race condition was addressed with additional validation.
CVE-2022-22622	Markup	A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions.	This issue was addressed with improved checks.
CVE-2022-22670	MediaRemote	A malicious application may be able to identify what other applications a user has installed.	An access issue was addressed with improved access restrictions.
CVE-2022-22672	MobileAccessoryUpdater	A malicious application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved memory handling.
CVE-2022-22659	NetworkExtension	An attacker in a privileged network position may be able to leak sensitive user information.	A logic issue was addressed with improved state management.
CVE-2022-22618	Phone	A user may be able to bypass the Emergency SOS passcode prompt.	This issue was addressed with improved checks.
CVE-2022-22609	Preferences	A malicious application may be able to read other applications' settings.	The issue was addressed with additional permissions checks.
CVE-2022-22600	Sandbox	A malicious application may be able to bypass certain Privacy preferences.	The issue was addressed with improved permissions logic.
CVE-2022-22599	Siri	A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen.	A permissions issue was addressed with improved validation.
CVE-2022-22639	SoftwareUpdate	An application may be able to gain elevated privileges.	A logic issue was addressed with improved state management.

CVE-2022-22621	UIKit	A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions.	This issue was addressed with improved checks.
CVE-2022-22671	VoiceOver	A person with physical access to an iOS device may be able to access photos from the lock screen.	An authentication issue was addressed with improved state management.
CVE-2022-22662	WebKit	Processing maliciously crafted web content may disclose sensitive user information.	A cookie management issue was addressed with improved state management.
CVE-2022-22610	WebKit	Processing maliciously crafted web content may lead to code execution	A memory corruption issue was addressed with improved state management.
CVE-2022-22624	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2022-22628	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2022-22629	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A buffer overflow issue was addressed with improved memory handling.
CVE-2022-22637	WebKit	A malicious website may cause unexpected cross-origin behavior.	A logic issue was addressed with improved state management.
CVE-2022-22668	Wi-Fi	A malicious application may be able to leak sensitive user information.	A logic issue was addressed with improved restrictions.
CVE-2022-22668	Wi-Fi	A malicious application may be able to leak sensitive user information.	A logic issue was addressed with improved restrictions.

Table 5: Vulnerabilities fixed in iOS 15.4.1

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-22675	AppleAVD	An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	An out-of-bounds write issue was addressed with improved bounds checking.

Table 6: Vulnerabilities fixed in iOS 15.5

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-26702	AppleAVD	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-26751	AppleGraphicsControl	Processing a maliciously crafted image may lead to arbitrary code execution.	A memory corruption issue was addressed with improved input validation.
CVE-2022-26736	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-26737	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2022-26738	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-26739	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-26740	AVEVideoEncoder	An application may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-26763	DriverKit	A malicious application may be able to execute arbitrary code with system privileges.	An out-of-bounds access issue was addressed with improved bounds checking.
CVE-2022-26744	GPU Drivers	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved state management.
CVE-2022-26711	ImageIO	A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	An integer overflow issue was addressed with improved input validation.
CVE-2022-26701	IOKit	An application may be able to execute arbitrary code with kernel privileges.	A race condition was addressed with improved locking.
CVE-2022-26768	IOMobileFrameBuffer	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved state management.
CVE-2022-26771	IOSurfaceAccelerator	A malicious application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved state management.
CVE-2022-26714	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved validation.
CVE-2022-26757	Kernel	An application may be able to execute arbitrary code with kernel privileges.	A use after free issue was addressed with improved memory management.
CVE-2022-26764	Kernel	An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	A memory corruption issue was addressed with improved validation.
CVE-2022-26765	Kernel	A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	A race condition was addressed with improved state handling.
CVE-2022-26706	LaunchServices	A sandboxed process may be able to circumvent sandbox restrictions.	An access issue was addressed with additional sandbox restrictions on third-party applications.
CVE-2022-23308	libxml2	A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2022-22673	Notes	Processing a large input may lead to a denial of service.	This issue was addressed with improved checks.
CVE-2022-26731	Safari Private Browsing	A malicious website may be able to track users in Safari private browsing mode.	A logic issue was addressed with improved state management.
CVE-2022-26766	Security	A malicious app may be able to bypass signature validation.	A certificate parsing issue was addressed with improved checks.
CVE-2022-26703	Shortcuts	A person with physical access to an iOS device may be able to access photos from the lock screen.	An authorization issue was addressed with improved state management.
CVE-2022-26700	WebKit	Processing maliciously crafted web content may lead to code execution.	A memory corruption issue was addressed with improved state management.
CVE-2022-26709	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution	A use after free issue was addressed with improved memory management.
CVE-2022-26710	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution	A use after free issue was addressed with improved memory management.
CVE-2022-26717	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution	A use after free issue was addressed with improved memory management.

CVE-2022-26716	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A memory corruption issue was addressed with improved state management.
CVE-2022-26719	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A memory corruption issue was addressed with improved state management.
CVE-2022-22677	WebRTC	Video self-preview in a webRTC call may be interrupted if the user answers a phone call.	A logic issue in the handling of concurrent media was addressed with improved state handling.
CVE-2022-26745	Wi-Fi	A malicious application may disclose restricted memory.	A memory corruption issue was addressed with improved validation.
CVE-2022-26760	Wi-Fi	A malicious application may be able to elevate privileges.	A memory corruption issue was addressed with improved state management.
CVE-2015-4142	Wi-Fi	A remote attacker may be able to cause a denial of service.	This issue was addressed with improved checks.
CVE-2022-26762	Wi-Fi	A malicious application may be able to execute arbitrary code with system privileges.	A memory corruption issue was addressed with improved memory handling.

Table 7: Vulnerabilities fixed in iOS 15.6

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-32832	APFS	An app with root privileges may be able to execute arbitrary code with kernel privileges.	The issue was addressed with improved memory handling.
CVE-2022-32788	AppleAVD	A remote user may be able to cause kernel code execution.	A buffer overflow was addressed with improved bounds checking.
CVE-2022-32824	AppleAVD	An app may be able to disclose kernel memory.	The issue was addressed with improved memory handling.
CVE-2022-32826	AppleMobileFileIntegrity	An app may be able to gain root privileges.	An authorization issue was addressed with improved state management.
CVE-2022-32845	Apple Neural Engine	An app may be able to break out of its sandbox.	This issue was addressed with improved checks.
CVE-2022-32840	Apple Neural Engine	An app may be able to execute arbitrary code with kernel privileges.	This issue was addressed with improved checks.
CVE-2022-32829	Apple Neural Engine	An app may be able to execute arbitrary code with kernel privileges.	This issue was addressed with improved checks.
CVE-2022-32810	Apple Neural Engine	An app may be able to execute arbitrary code with kernel privileges.	The issue was addressed with improved memory handling.
CVE-2022-32820	Audio	An app may be able to execute arbitrary code with kernel privileges.	An out-of-bounds write issue was addressed with improved input validation.
CVE-2022-32825	Audio	An app may be able to disclose kernel memory.	The issue was addressed with improved memory handling.
CVE-2022-32828	CoreMedia	An app may be able to disclose kernel memory.	The issue was addressed with improved memory handling.
CVE-2022-32839	CoreText	A remote user may cause an unexpected app termination or arbitrary code execution.	The issue was addressed with improved bounds checks.
CVE-2022-32819	File System Events	An app may be able to gain root privileges.	A logic issue was addressed with improved state management.
CVE-2022-32793	GPU Drivers	An app may be able to disclose kernel memory.	Multiple out-of-bounds write issues were addressed with improved bounds checking.
CVE-2022-32821	GPU Drivers	An app may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved validation.
CVE-2022-32855	Home	A user may be able to view restricted content from the lock screen.	A logic issue was addressed with improved state management.
CVE-2022-32849	iCloud Photo Library	An app may be able to access sensitive user information.	An information disclosure issue was addressed by removing the vulnerable code.

CVE-2022-32787	ICU	Processing maliciously crafted web content may lead to arbitrary code execution.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-32841	ImageIO	Processing a maliciously crafted image may result in disclosure of process memory.	The issue was addressed with improved memory handling.
CVE-2022-32802	ImageIO	Processing a maliciously crafted file may lead to arbitrary code execution.	A logic issue was addressed with improved checks.
CVE-2022-32830	ImageIO	Processing a maliciously crafted image may lead to disclosure of user information.	An out-of-bounds read issue was addressed with improved bounds checking.
CVE-2022-32785	ImageIO	Processing an image may lead to a denial-of-service.	A null pointer dereference was addressed with improved validation.
CVE-2022-26768	IOMobileFrameBuffer	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved state management.
CVE-2022-32813	Kernel	An app with root privileges may be able to execute arbitrary code with kernel privileges.	The issue was addressed with improved memory handling.
CVE-2022-32815	Kernel	An app with root privileges may be able to execute arbitrary code with kernel privileges.	The issue was addressed with improved memory handling.
CVE-2022-32817	Kernel	An app may be able to disclose kernel memory.	An out-of-bounds read issue was addressed with improved bounds checking.
CVE-2022-32844	Kernel	An app with arbitrary kernel read and write capability may be able to bypass Pointer Authentication.	A logic issue was addressed with improved state management.
CVE-2022-32844	Kernel	An app with arbitrary kernel read and write capability may be able to bypass Pointer Authentication.	A race condition was addressed with improved state handling.
CVE-2022-26981	Liblouis	An app may cause unexpected app termination or arbitrary code execution.	This issue was addressed with improved checks.
CVE-2022-32823	libxml2	An app may be able to leak sensitive user information.	A memory initialization issue was addressed with improved memory handling.
CVE-2022-32814	Multi-Touch	An app may be able to execute arbitrary code with kernel privileges.	A type confusion issue was addressed with improved state handling.
CVE-2022-32838	PluginKit	An app may be able to read arbitrary files.	A logic issue was addressed with improved state management.
CVE-2022-32784	Safari Extensions	Visiting a maliciously crafted website may leak sensitive data.	The issue was addressed with improved UI handling.
CVE-2022-32857	Software Update	A user in a privileged network position can track a user's activity.	This issue was addressed by using HTTPS when sending information over the network.
CVE-2022-32816	WebKit	Visiting a website that frames malicious content may lead to UI spoofing.	The issue was addressed with improved UI handling.
CVE-2022-32792	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	An out-of-bounds write issue was addressed with improved input validation.
CVE-2022-2294	WebRTC	Processing maliciously crafted web content may lead to arbitrary code execution.	A memory corruption issue was addressed with improved state management.
CVE-2022-32837	Wi-Fi	An app may be able to cause unexpected system termination or write kernel memory.	This issue was addressed with improved checks.
CVE-2022-32847	Wi-Fi	A remote user may be able to cause unexpected system termination or corrupt kernel memory.	This issue was addressed with improved checks.

Table 8: Vulnerabilities fixed in iOS 15.6.1

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-32894	Kernel	An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-32893	WebKit	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.	An out-of-bounds write issue was addressed with improved bounds checking.

Table 9: Vulnerabilities fixed in iOS 15.7

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-32854	Contacts	An app may be able to bypass Privacy preferences.	This issue was addressed with improved checks.
CVE-2022-32911	Kernel	An app may be able to execute arbitrary code with kernel privileges.	The issue was addressed with improved memory handling.
CVE-2022-32864	Kernel	An app may be able to disclose kernel memory.	The issue was addressed with improved memory handling.
CVE-2022-32917	Kernel	An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	The issue was addressed with improved bounds checks.
CVE-2022-32883	Maps	An app may be able to read sensitive location information.	A logic issue was addressed with improved restrictions.
CVE-2022-32908	MediaLibrary	A user may be able to elevate privileges.	A memory corruption issue was addressed with improved input validation.
CVE-2022-32795	Safari	Visiting a malicious website may lead to address bar spoofing.	This issue was addressed with improved checks.
CVE-2022-32868	Safari Extensions	A website may be able to track users through Safari web extensions.	A logic issue was addressed with improved state management.
CVE-2022-32872	Shortcuts	A person with physical access to an iOS device may be able to access photos from the lock screen.	A logic issue was addressed with improved restrictions.
CVE-2022-32886	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	A buffer overflow issue was addressed with improved memory handling.
CVE-2022-32912	WebKit	Processing maliciously crafted web content may lead to arbitrary code execution.	An out-of-bounds read was addressed with improved bounds checking.

Table 10: Vulnerabilities fixed in iOS 15.7.1

Vulnerability ID	Component	Impact	Mitigation
CVE-2022-32932	Apple Neural Engine	An app may be able to execute arbitrary code with kernel privileges	The issue was addressed with improved memory handling.
CVE-2022-42798	Audio	Parsing a maliciously crafted audio file may lead to disclosure of user information	The issue was addressed with improved memory handling.

CVE-2022-32929	Backup	An app may be able to access iOS backups	A permissions issue was addressed with additional restrictions.
CVE-2022-32935	FaceTime	A user may be able to view restricted content from the lock screen	A lock screen issue was addressed with improved state management.
CVE-2022-32939	Graphics Driver	An app may be able to execute arbitrary code with kernel privileges	The issue was addressed with improved bounds checks.
CVE-2022-32949	Image Processing	An app may be able to execute arbitrary code with kernel privileges	This issue was addressed with improved checks.
CVE-2022-32944	Kernel	An app may be able to execute arbitrary code with kernel privileges	A memory corruption issue was addressed with improved state management.
CVE-2022-42803	Kernel	An app may be able to execute arbitrary code with kernel privileges	A race condition was addressed with improved locking.
CVE-2022-32926	Kernel	An app with root privileges may be able to execute arbitrary code with kernel privileges	The issue was addressed with improved bounds checks.
CVE-2022-42827	Kernel	An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	An out-of-bounds write issue was addressed with improved bounds checking.
CVE-2022-42801	Kernel	An app may be able to execute arbitrary code with kernel privileges	A logic issue was addressed with improved checks.
CVE-2022-42810	Model I/O	Processing a maliciously crafted USD file may disclose memory contents	The issue was addressed with improved memory handling.
CVE-2022-32941	ppp	A buffer overflow may result in arbitrary code execution	The issue was addressed with improved bounds checks.
CVE-2022-42817	Safari	Visiting a maliciously crafted website may leak sensitive data	A logic issue was addressed with improved state management.
CVE-2022-32923	WebKit	Processing maliciously crafted web content may disclose internal states of the app	A correctness issue in the JIT was addressed with improved checks.
CVE-2022-32927	Wi-Fi	Joining a malicious Wi-Fi network may result in a denial-of-service of the Settings app	The issue was addressed with improved memory handling.
CVE-2022-37434	zlib	A user may be able to cause unexpected app termination or arbitrary code execution	This issue was addressed with improved checks.
CVE-2022-42800	zlib	A user may be able to cause unexpected app termination or arbitrary code execution	This issue was addressed with improved checks.