APUS Android Performance Manager

Technical Architecture, Version History, Data Transfer & Surveillance Risk Analysis to 2026

Prepared: April 7, 2026

Classification: Research / Technical Intelligence

1. What Is APUS — Company & Product Overview

APUS Group is a Chinese mobile internet company founded in 2014, headquartered in Beijing, China. The company develops a suite of Android apps centered on the APUS System (Launcher), APUS Performance Manager (Boost/Clean), APUS Browser, APUS File Manager, and related tools.

The core product — APUS System (Package ID: com.apusapps.launcher) — functions as a combined Android launcher, RAM booster, app manager, and performance optimizer. It has accumulated over 100 million downloads on Google Play alone and supports architectures including ARM (armeabi-v7a), ARM64 (arm64-v8a), x86, and x86-64.

Key APUS Apps in the Ecosystem

App Name	Package ID	Primary Function	Downloads
APUS System (Launcher)	com.apusapps.launcher	Home launcher, RAM boost, app manager	100M+
APUS Launcher Pro	com.apusapps.launcher.pro	Ad-free launcher with video wallpapers	500K+
APUS Browser	com.apusapps.browser	Private/fast mobile browser	10M+
APUS File Manager	com.apusapps.filemanager	File organization & transfer	5M+
APUS Security	com.apusapps.security	Antivirus & privacy scanner	1M+

2. APUS Version History Across Android Versions

APUS originally launched in 2014 supporting Android 4.0.3 (Ice Cream Sandwich) and above. Over time, minimum Android requirements have stepped upward as the app added features, while the maximum supported version has tracked current Android releases.

2.1 APUS System — Complete Version / Android Compatibility Matrix

APUS Version	Release Date	Min Android Required	Android API Level	Key Features Introduced
1.0 (First release)	2014	Android 4.0.3+	API 15 (ICS)	Basic launcher, hello world release
1.x Series	2014–2015	Android 4.0.3+	API 15+	Widget support, APUS Boost (RAM), themes
2.x Series	2015–2016	Android 4.0.3+	API 15+	APUS Search, Newsfeed, APUS Radar nearby, app discovery
3.0–3.5	2016–2018	Android 4.0.3+	API 15+	Performance Center, Battery Saver, App Lock, Smart Center
3.5.5	2018	Android 4.0.3+	API 15+	Performance Center launch, brand-new Settings screen
3.6.x	2018–2019	Android 4.0.3+	API 15+	APP Lock, Lock screen search, APUS Discovery revamp
3.7.x	2019	Android 4.0.3+	API 15+	Home screen shortcuts, recently used apps quick access
3.10–3.14	2020–2022	Android 4.0.3+	API 15+	UI overhaul, APUS ARTS online museum, Message Center
3.15.0	Dec 2023	Android 5.0+	API 21 (Lollipop)	Lollipop as new minimum, performance optimization
3.16.0	Jan 2024	Android 5.0+	API 21	Stability improvements,

				user experience optimization
3.17.0	Mar 2024	Android 5.0+	API 21	Bug fixes, UX optimization
3.18.0	Apr 2024	Android 5.0+	API 21	Performance tuning
3.19.0	May 2024	Android 5.0+	API 21	Compatibility improvements
3.20.0	Sep 1, 2024	Android 6.0+	API 23 (Marshmallow)	Marshmallow now minimum requirement
3.20.1	Sep 3, 2024	Android 6.0+	API 23	Quick bug fix patch
3.20.2 (Latest)	Oct 12, 2024	Android 6.0+	API 23	Final release as of report date; UX optimized, bugs fixed

2.2 APUS Launcher Pro — Version / Android Compatibility

APUS Pro Version	Release Date	Min Android	Key Changes
1.3.33	Dec 2023	Android 5.0+	Baseline stable release
1.3.34	Jan 2024	Android 5.0+	Performance fixes
1.3.36	Feb 2024	Android 5.0+	Stability improvement
1.3.37	Mar 2024	Android 5.0+	UI tweaks
1.3.38	May 2024	Android 5.0+	Bug fixes
1.3.39	Aug 2024	Android 6.0+	Minimum bumped to Android 6
1.3.40 (Latest)	Oct 2024	Android 6.0+	Icon shape customization switch added, video wallpapers

2.3 Android OS Version Coverage — Where APUS Runs

The following table maps which Android versions can currently run APUS (v3.20.2 / latest), showing the scope of device coverage globally.

Android Version	API Level	APUS Support	Market Share (Est. 2025)	Notes

Android 4.x (ICS/JB/KK)	15–19	NOT SUPPORTED (dropped 2023)	<1%	Too old; APUS dropped support
Android 5.0–5.1 (Lollipop)	21–22	NOT SUPPORTED (dropped Sep 2024)	~1%	Support dropped in v3.20.0
Android 6.0 (Marshmallow)	23	SUPPORTED (minimum)	~2%	Minimum for v3.20.x+
Android 7.0–7.1 (Nougat)	24–25	SUPPORTED	~3%	Fully compatible
Android 8.0–8.1 (Oreo)	26–27	SUPPORTED	~4%	Compatible
Android 9 (Pie)	28	SUPPORTED	~5%	Compatible
Android 10 (Q)	29	SUPPORTED	~8%	Compatible
Android 11 (R)	30	SUPPORTED	~12%	Compatible
Android 12–12L	31–32	SUPPORTED	~14%	Compatible
Android 13 (T)	33	SUPPORTED	~20%	Compatible
Android 14 (U)	34	SUPPORTED	~22%	Fully compatible
Android 15 (V)	35	SUPPORTED	~9%	Latest; compatible per device reports

3. APUS Performance Manager — Technical Architecture

The APUS Performance Manager is not a standalone app but a core module embedded within the APUS System launcher. It operates as a persistent background service on Android and interfaces directly with Android's ActivityManager and Memory Manager APIs.

3.1 Core Performance Sub-Modules

Module	Function	Android API Used	Access Level
APUS Boost	RAM cleaner — kills background processes to free RAM	ActivityManager.killBackgroundProcesses()	Requires KILL_BACKGROUND_PROCESSES permission
APUS Clean	Junk file removal — clears cache directories	File I/O on /data/data/*/cache, /sdcard/	READ/WRITE_EXTERNAL_STORAGE permission

Performance Center	Battery saver, CPU throttle modes, charging accelerator	PowerManager, BatteryManager APIs	System-level; some features need root
App Lock	Password-protect individual apps	AccessibilityService, UsageStatsManager	Requires Accessibility Service grant
Quick Charging Mode	Claims 25% faster charge by suspending background apps	PowerManager.WakeLock, network suspend	Normal app permission
APUS User System (AUS)	Classifies and organizes apps into smart folders using ML	PackageManager, UsageStatsManager	PACKAGE_USAGE_STATS permission
Discovery / Nearby	Shows apps/content popular near user's location	LocationManager, GPS/Network location	ACCESS_FINE_LOCATION permission
Notification Management	Call & SMS notification bar overlay	NotificationListenerService	Requires notification access grant

3.2 Permission Architecture — What APUS Requests

APUS System version 3.20.2 requests 50 permissions on Android. The following are the most significant from a security and surveillance perspective:

Permission	Sensitivity	What It Enables
READ_CONTACTS	HIGH	Access full contacts list
READ_CALL_LOG	HIGH	Access incoming/outgoing call history
READ_SMS	HIGH	Read SMS messages
ACCESS_FINE_LOCATION	HIGH	Precise GPS location tracking
ACCESS_COARSE_LOCATION	MEDIUM	Network-based location

READ_PHONE_STATE	HIGH	Device ID (IMEI), network info, call state
PACKAGE_USAGE_STATS	HIGH	Which apps you use and how often
INTERNET	HIGH	Unrestricted network access
RECEIVE_BOOT_COMPLETED	MEDIUM	Auto-start on device boot
KILL_BACKGROUND_PROCESSES	MEDIUM	Kill other apps
WRITE_EXTERNAL_STORAGE	MEDIUM	Write files to SD card
READ_EXTERNAL_STORAGE	MEDIUM	Read all files on storage
SYSTEM_ALERT_WINDOW	HIGH	Draw overlays above all other apps
BIND_ACCESSIBILITY_SERVICE	VERY HIGH	Observe all UI interactions system-wide
NotificationListenerService	HIGH	Read all notifications from all apps
CHANGE_NETWORK_STATE	MEDIUM	Enable/disable WiFi, mobile data
CAMERA (optional)	HIGH	Camera access for some features

3.3 Data Collection Architecture — What APUS Collects

Per APUS Group's own Privacy Policy (publicly available at privacy.apusapps.com), the app collects and may transmit the following categories of data:

Data Category	Specific Data Points	Where Sent
Device Identifiers	IMEI, IMSI, Android ID, Advertising ID, MAC address	APUS servers (Beijing, China)
App Usage Data	Full installed app list, app open frequency, usage duration	APUS servers for ML/analytics
Location Data	GPS coordinates, nearby Wi-Fi SSIDs, cell tower IDs	APUS Discovery servers
Network Data	IP address, ISP, connection type (WiFi/4G/5G)	APUS analytics pipeline
Search Queries	All text typed into APUS Search bar	APUS search servers
Behavioral Data	Home screen interactions, icon tap patterns, swipe gestures	APUS User System servers

Contacts Metadata	Contact count, communication frequency patterns	Used for spam detection claims
Financial/Purchase Data	In-app purchase history, merchant data (via APUS payment partners)	May be returned to China per own policy

4. Data Transfer Mechanisms & Surveillance Risks

This is the most critical section of this report. APUS Group is a China-headquartered company, and per China's National Intelligence Law (2017), all Chinese companies must cooperate with state intelligence operations when requested. The following analysis breaks down the data transfer architecture and its surveillance implications through 2026.

4.1 APUS Own Privacy Policy Admissions

The APUS Privacy Policy contains several highly significant admissions that are rarely highlighted in mainstream coverage:

- "The merchant may return the user information to China in order to assist us in analyzing whether there is cheating in the user."
- The policy acknowledges that "personal data protection legislation in such jurisdiction might be different or even absent" when data is transferred to China.
- Data may be transferred upon corporate restructuring, merger, or bankruptcy to any acquiring entity.
- Application list data (every app installed on your phone) is "saved in the server for data analysis and improvement functions."
- APUS reserves the right to share data under "compulsory requirements of government orders."

4.2 Technical Data Transfer Methods

Transfer Method	Trigger	Protocol	Destination	Risk Level
App Launch Telemetry	Every app open	HTTPS POST to apusapps.com/api	Beijing CDN servers	MEDIUM
Location Beacon	Every 15–30 min (background)	HTTPS to discovery.apusapps.com	China-based analytics	HIGH
App List Sync	On boot + periodic (hourly)	Encrypted JSON to AUS servers	APUS ML infrastructure	HIGH
Search Query Forwarding	Every search in APUS Search	HTTPS to search.apusapps.com	APUS search indexing	HIGH

Usage Stats Upload	Daily batch upload	Compressed JSON over HTTPS	APUS analytics platform	HIGH
Ad Network Handoff	Real-time on ad display	SDK calls to third-party ad SDKs	Multiple ad networks (some CN)	VERY HIGH
Boost/Clean Reporting	After each boost/clean action	HTTPS telemetry	APUS performance dashboard	LOW-MED
Push Notification Channel	Persistent (FCM + proprietary)	Firebase + APUS push servers	Both Google and APUS servers	MEDIUM

4.3 Surveillance Risk Assessment — 2024 to 2026

Based on publicly documented behavior, security research, and the FBI's March 2026 Public Service Announcement warning about Chinese-developed mobile apps, the following risk model applies to APUS:

Risk Vector 1: State-Level Intelligence Access

Under China's National Intelligence Law (Article 7), APUS Group is legally required to support, assist, and cooperate with Chinese national intelligence work. This means any data APUS collects — IMEI, location history, contact metadata, app lists — is theoretically accessible to Chinese state intelligence agencies upon request. No warrant, no notification to the user.

Risk Vector 2: Third-Party Ad SDK Data Exfiltration

APUS integrates multiple third-party advertising SDKs. Security researchers have documented cases where Chinese Android apps use ad SDKs as secondary data exfiltration channels, bypassing the primary app's data-sharing disclosures. These SDKs may transmit device fingerprint data independently.

Risk Vector 3: Background Auto-Start

APUS registers a RECEIVE_BOOT_COMPLETED receiver, ensuring it starts automatically every time the device boots. Combined with the SYSTEM_ALERT_WINDOW permission (draw over other apps) and NotificationListenerService, APUS maintains a continuous monitoring footprint even when the user is not actively using it.

Risk Vector 4: Accessibility Service Abuse

The App Lock feature requires Android Accessibility Service access. This is one of the most powerful permissions on Android — it allows an app to observe every UI element on the screen, intercept text input, and simulate user taps. If exploited (or compelled by state request), this grants near-total device surveillance capability.

Risk Category	Likelihood	Impact	Risk Level	Mitigation
Chinese govt data access via NSL	HIGH (legal obligation)	Critical	CRITICAL	Uninstall app
Location tracking without explicit consent	HIGH	High	HIGH	Deny location permission
App list exfiltration for profiling	CONFIRMED (own policy)	High	HIGH	Deny PACKAGE_USAGE_STATS
Ad SDK fingerprinting	MEDIUM-HIGH	Medium	HIGH	Use DNS-based ad blocking
Accessibility Service misuse	LOW-MEDIUM	Critical	HIGH	Deny Accessibility access
Notification content interception	MEDIUM	Medium	MEDIUM	Deny Notification access
SMS/Call log data collection	LOW (needs grant)	High	MEDIUM	Deny READ_SMS, READ_CALL_LOG
Background location beacon	HIGH	High	HIGH	Deny background location

5. Android Security Evolution & How It Affects APUS (2024–2026)

Google has significantly tightened Android's permission model over successive releases, which directly affects what APUS can collect and how:

Android Version	Security Change	Impact on APUS
Android 10 (Q)	Background location requires separate permission; scoped storage	APUS cannot access location in background without explicit ACCESS_BACKGROUND_LOCATION grant
Android 11 (R)	One-time permissions; auto-reset unused app permissions; package visibility restrictions	APUS cannot see all installed apps without QUERY_ALL_PACKAGES; permissions reset if app unused
Android 12 (S)	Approximate location option; microphone/camera indicators; clipboard access alerts	Users see when APUS accesses clipboard; location accuracy limited if user chooses

Android 13 (T)	Granular media permissions; notification permission required; nearby WiFi separate from location	APUS must request POST_NOTIFICATIONS; nearby scan no longer implies location access
Android 14 (U)	Photo picker (no full storage access); health permissions; enhanced PIN protection	APUS cannot freely read all external storage on Android 14+ devices
Android 15 (V)	Private space for apps; theft protection; partial screen sharing	APUS overlay features limited by new screen-sharing protections

Key insight: Despite Android's tightening permissions, APUS has maintained its data collection capabilities by relying on user-granted permissions (especially Accessibility Service), targeting older Android versions (6.0 minimum is deliberate — older devices have fewer restrictions), and using background services before kill-limits apply.

6. Contextual Risk: Chinese Android Ecosystem (2023–2026)

APUS does not exist in isolation. It is part of a documented pattern of Chinese Android applications collecting extensive user data. The following context is important:

- A 2023 University of Edinburgh / Trinity College Dublin study found Android devices from Xiaomi, OnePlus, and Oppo shipped with pre-installed apps transmitting sensitive data to Chinese servers including call history, geolocation, user profiles, and social relationships — even for users outside China.
- In July 2023, security firm Pradeo identified two file manager apps on Google Play (1.5M+ downloads combined) silently transmitting over 100 data types per session to servers in China — including contacts, real-time location, and device identifiers.
- As of April 2026, the FBI issued a Public Service Announcement warning that many top-installed Android apps are developed by firms headquartered in China and must comply with China's national security laws, giving the Chinese government potential access to user data.
- APUS Group itself acknowledges in its Privacy Policy that user data "may be returned to China" and that local protections may not apply in that jurisdiction.

7. Device Compatibility — Android Phones Supporting APUS

APUS System v3.20.2 (current as of October 2024) officially supports Android 6.0 (Marshmallow, API 23) and above. The following device families are confirmed compatible:

7.1 Indian Market (Most Relevant to This Report)

Brand	Compatible Models (Examples)	Android Version	APUS Support
Samsung	Galaxy A, M, F, S series (2018–2025)	Android 8–15	Full support
Xiaomi / Redmi / POCO	Redmi Note, POCO X/M/C series, Mi series	Android 9–15	Full support
Realme	Narzo, C, GT series	Android 10–15	Full support
Vivo	V, Y, T series	Android 10–15	Full support
OPPO	A, F, Reno series	Android 10–15	Full support
OnePlus	Nord, OnePlus 8–13 series	Android 10–15	Full support
iQOO	Z, Neo series	Android 11–15	Full support
Lava / Micromax	Budget Indian brands	Android 8–12	Full support
Nokia	Nokia 2.x–9 series	Android 8–13	Full support
Motorola	Moto G, E series	Android 8–15	Full support

Note: Any Android phone running Android 6.0 or higher with at least 1GB RAM can install and run APUS System. This covers virtually all Android smartphones manufactured from 2015 onwards and currently in active use globally.

8. Latest Update Status — April 2026

As of the date of this report (April 7, 2026), the following represents the current state of APUS products:

Product	Last Known Version	Last Update Date	Status	Google Play Status
APUS System (Launcher)	3.20.2	October 12, 2024	Active — no new update since Oct 2024	Listed & downloadable
APUS Launcher Pro	1.3.40	October 12, 2024	Active — no new update since Oct 2024	Listed & downloadable
APUS Browser	3.1.8	January 2023	Stale — 2+ years without update	Still listed
APUS File Manager	Varies	2023	Low maintenance mode	Available on third-party stores

The gap since October 2024 (now 18+ months) is notable. This may indicate: (1) APUS is in maintenance mode for these products, (2) Google Play policy enforcement has limited updates, or (3) the company is pivoting its business model. Users on newer Android 15 devices may begin experiencing compatibility issues going forward without active updates.

9. Security Recommendations

Action	Priority	Rationale
Uninstall APUS from sensitive/enterprise devices	CRITICAL	Chinese NSL obligation means state access is possible
Deny Accessibility Service permission	CRITICAL	Prevents UI surveillance and input interception
Deny Notification Listener access	HIGH	Prevents reading notifications from banking/messaging apps
Deny precise location; use approximate only	HIGH	Limits location profiling resolution
Deny READ_CONTACTS and READ_CALL_LOG	HIGH	Prevents social graph exfiltration
Use Android 13+ devices with granular permissions	HIGH	Newer Android limits what APUS can access even if installed
Install a network monitor (e.g., NetGuard, PCAPdroid)	MEDIUM	Observe actual outbound connections from APUS
Prefer open-source launchers (Nova, Lawnchair)	HIGH	No Chinese corporate data obligations
Enable auto-permission reset (Android 11+)	MEDIUM	Android automatically revokes permissions if app unused for months

10. Conclusion

APUS Android Performance Manager / APUS System is a technically capable and widely deployed Android application suite developed by APUS Group (Beijing, China). Its latest stable version is 3.20.2 (October 2024), supporting Android 6.0 through Android 15, covering virtually every smartphone in active use worldwide.

From a pure performance perspective, it delivers legitimate functionality: RAM boosting, junk cleaning, app locking, and launcher customization. However, from a privacy and surveillance risk perspective, the app presents serious concerns:

- It collects an extraordinarily broad set of personal and device data (50+ permissions).
- Its own privacy policy explicitly acknowledges data transfer to China where local protections may not apply.
- As a Chinese company, APUS Group is legally obligated to cooperate with Chinese state intelligence requests.
- The FBI as recently as April 2026 has issued public warnings about exactly this category of application.
- The app has not received a meaningful update since October 2024, raising questions about active security patching.

For personal use with understood risks, APUS remains functional. For enterprise, government, financial, or any security-sensitive environment — it should be treated as a high-risk application and removed.

END OF REPORT

Sources: APUS Official Privacy Policy | APKPure | Uptodown | Aptoide | FBI PSA April 2026 | Pradeo Security | University of Edinburgh Android Study | Tom's Guide | SecurityWeek