MEDIA RELEASE

For Immediate Release

BYD AUSTRALIA RESPONDS TO FOUR CORNERS' CLAIMS OF VEHICLE CYBERSECURITY BREACH

01 October, 2026

BYD Australia today responded to claims made by the Four Corners program on 21 September concerning the cybersecurity of a Shark 6 vehicle.

BYD took the claims extremely seriously, prompting an immediate and through forensic investigation involving technical teams in Australia and China.

The investigation focused on two areas: a breach of the vehicle's infotainment software system through the Android Debug Bridge[1] (ADB), and physical access to the vehicle's CAN bus by tapping directly into the vehicle wiring.

Regarding the infotainment system. The ADB is disabled by default and can only be accessed by authorised persons using special tools. The researcher exploited a software defect to enable the ADB and subsequently install an untrusted third-party application.

BYD engineers in their investigation were able to reproduce both the software defect used to enable ADB and the subsequent installation of an untrusted third-party application. When the application requested access to certain information or functions, such as the vehicle's location or microphone, the infotainment system displayed a permission prompt. The requested permissions could only be granted after the user manually approved the request through the infotainment interface.

Regarding the CAN bus. BYD's technical analysis has confirmed that the demonstrated control of the vehicle's headlights and windscreen wipers required direct physical access to the vehicle's internal CAN bus by tapping into the vehicle wiring.

This method requires physical intervention on the target vehicle and is limited to the individual vehicle that has been physically accessed.

Without physically tapping into the vehicle wiring, an external device seeking to access the relevant vehicle network through the diagnostic interface would need to do so via the On-Board Diagnostics (OBD) interface.

BYD has implemented security measures for the OBD interface, including device authentication and physical isolation, and has established corresponding cybersecurity safeguards in accordance with the requirements of UN R155.

BYD Internal Actions

For the confirmed ADB-related software issue, BYD has completed the root-cause investigation and commenced software remediation.

The corrective action will address the identified ADB-related software issue and remove the unintended pathway that allows ADB to be enabled through the infotainment system user interface, thereby eliminating the access path identified during the investigation.

The updated software will be deployed as part of a future Over the Air (OTA) infotainment system software update for Shark 6 vehicles, and only once the updated software has undergone rigorous validation. BYD is also investigating if the software update is required for other BYD vehicles sold in Australia.

Regarding CAN bus cybersecurity. BYD has also initiated a dedicated risk assessment. This assessment will evaluate the necessity and technical feasibility of additional measures relating to CAN message authenticity, integrity and freshness verification. Any further technical improvements will be determined based on the outcome of this assessment.

In addition, BYD will use the findings to further review and strengthen relevant cybersecurity controls and development processes, including debug-interface management, application permission control, pre-release cybersecurity testing, vulnerability management, and cross-platform issue screening.

BYD remains committed to enhancing cybersecurity protection throughout the vehicle lifecycle through ongoing vulnerability analysis, security testing, risk assessment and software updates.

1 ADB (Android Debug Bridge) is a command-line debugging tool provided as part of the Android system. It enables communication with a host device via USB or TCP/IP and is commonly used for functions such as Android Package Kit installation, log collection, file transfer, application debugging, and performance analysis. ADB is a standard Android capability and is not proprietary to BYD. BYD does not design the underlying ADB functionality; rather, it uses this Android-provided capability during development and debugging activities. In the production configuration, ADB is disabled by default.

...ends/

For all enquiries please contact:
Paul Ellis
BYD Australia Public Relations Director
e. paul.ellis@byd.com and p: 0455 344 431