AUTOMOTIVEPULSE.APP

Threat Feed Report

Generated 09 Nov 2026, 00:27 SGT
Matching stories: 5
Severity: high

---

1. Global Automotive Cyber Incidents/Events | HIGH

Hyundai and Kia will repair millions of vehicles under a deal to fix anti-theft technology

Wbrz | 08 Nov 2026, 05:31 SGT

Hyundai and Kia reached a nationwide settlement with 35 states, led by Minnesota Attorney General Keith Ellison, requiring free repairs to millions of vehicles that lacked engine immobilizers and were left vulnerable to theft. The remedy could cost the automakers over 500 million dollars, and all future US-sold vehicles must include immobilizers, with up to 4.5 million dollars in restitution for theft-damaged vehicles. The settlement addresses a well-documented design weakness exploited in viral theft challenges targeting keyless ignition models. Affected owners must obtain the free software and hardware remedy through dealers.

https://www.wbrz.com/videos/hyundai-and-kia-will-repair-millions-of-vehicles-under-a-deal-to-fix-anti-theft-technology/

---

2. Global Automotive Cyber Incidents/Events | HIGH

Japan’s cybersecurity nightmare also everyone else’s problem too | BusinessMirror

Businessmirror | 08 Nov 2026, 02:37 SGT

A February 2022 hack of Kojima Industries, a small supplier of cup holders, USB sockets and interior parts, forced Toyota to halt 14 factories at an estimated cost of about 375 million dollars. The incident illustrates how a low-tier supplier with weak security can disrupt an entire OEM production network. Kojima took months to restore operations to near-normal levels, and the case sits within a broader wave of ransomware attacks on Japanese manufacturers. The event supports supply-chain security requirements and tiered assurance obligations for smaller automotive suppliers.

Affected Vehicle Make & Model: Toyota

Observed MITRE ATT&CK techniques: T1195 Supply Chain Compromise | T1486 Data Encrypted for Impact

https://businessmirror.com.ph/2023/04/23/japans-cybersecurity-nightmare-also-everyone-elses-problem-too/

---

3. Autonomous Vehicles (AV) | HIGH

Two Tesla Crashes on California’s Interstate 80 Leave Pedestrian Dead and Two Police Officers Seriously Injured as Full Self-Driving Faces Scrutiny - Travel And Tour World

Travelandtourworld | 07 Nov 2026, 23:22 SGT

Two Tesla crashes on California's Interstate 80 in Solano County on 13 and 22 October 2026 left one pedestrian dead and two police officers seriously injured, with both drivers reporting use of Tesla's Full Self-Driving system. The incidents intensify scrutiny of driver attention and advanced driver-assistance technology on major Northern California corridors.

Affected Vehicle Make & Model: Tesla

https://www.travelandtourworld.com/news/article/d56mvd5ftj8g/

---

4. Global Automotive Cyber Incidents/Events | HIGH

Researchers unlock automaker connected cars globally via | TLDR

Tldr | 07 Nov 2026, 18:56 SGT

Researchers found vulnerabilities in a major automaker's connected car platform enabling remote unlocking and control of vehicles in Australia and other regions. Exploiting exposed admin tools, identity credentials, and a firewall path traversal bypass let them mint app tokens and send remote commands, underscoring cybersecurity risk in connected vehicle fleets.

Observed MITRE ATT&CK techniques: T1078 Valid Accounts | T1190 Exploit Public-Facing Application | T1552 Unsecured Credentials

https://tldr.tech/story/eb9d855e-ce3f-4ede-aec6-d947c79a9c82

---

5. Global Automotive Cyber Incidents/Events | HIGH

Tata Motors Shares Rise 2% As JLR Restores Systems

Samco | 07 Nov 2026, 14:51 SGT

Jaguar Land Rover has begun a controlled, phased restoration of digital systems disrupted by a cyber attack, with sections of its digital estate back online and operations resuming in a managed manner. The incident affected JLR's manufacturing and retail-facing systems, and the recovery announcement lifted parent Tata Motors shares by over 2 percent after a two-day decline. The event underscores the operational and financial exposure automakers face from attacks on production and dealer networks. Recovery work remains ongoing, with suppliers and retail partners notified as systems return.

https://www.samco.in/knowledge-center/articles/tata-motors-shares-jump-2-as-jlr-recovers-systems-post-cyber-attack/
