LaLiga confirms fan data stolen from a fan-services platform



LaLiga says an attacker accessed one of its fan-services platforms between 14 and 16 November and extracted personal data of registered users, including users of some clubs' services. The league reports the incident was confined to that platform.

- The unauthorized access took place between 14 and 16 November; the security team identified its source on 16 November and moved to block it and stop the extraction.
- The affected data belongs to users registered for digital services offered by LaLiga and some clubs.
- LaLiga states the incident did not reach other systems that support the running of the competitions.
- The league reported the incident to the Spanish Data Protection Agency (AEPD) and filed a complaint with the National Police's Central Cybercrime Unit.

> - Affected clubs have been notified directly, and notification of fans is being coordinated; no ransomware group has claimed the attack so far.

LaLiga, the organizer of Spain's top two men's professional football divisions, has disclosed a breach of one of its technology platforms for fan services. The league says an attacker gained unauthorized access between 14 and 16 November and extracted personal data of users registered for digital services offered by LaLiga and some clubs.

What the league reports

On 16 November, LaLiga's security team identified the source of the access and put measures in place to block the attack and stop the data extraction. The league says the incident was limited to one platform and did not extend to the systems that support the running of the competitions.

After containment, LaLiga began an investigation to establish the scope of the incident and introduced more thorough monitoring to detect further attempts. It notified the Spanish Data Protection Agency (AEPD), filed a complaint with the National Police's Central Cybercrime Unit, and informed affected clubs directly. Communication to affected fans is being coordinated.

What is not yet known

The source does not specify which clubs or how many users are affected, or which data fields were taken. No ransomware group has claimed responsibility. BleepingComputer has asked LaLiga for more detail and had not received a response at publication.

Relevance for Saudi institutions

The case illustrates a familiar pattern: a customer-facing platform shared with partner organizations becomes the point of exposure for personal data. Institutions that run fan, customer or member portals, or that share user data with affiliates, can use this as a prompt to review their own arrangements.

What to do now

1. Inventory customer-facing platforms that hold personal data, including those shared with affiliates or partners, and confirm each has a named owner.
2. Check that these platforms are segmented from core operational systems, so a compromise stays contained as LaLiga reports was the case for it.
3. Review monitoring and logging on such platforms for unusual bulk data extraction, and confirm alerts reach the response team.
4. Test your personal-data breach procedure, including notification to the competent authority under the PDPL and to affected partners and individuals.

5. Confirm data-sharing agreements with affiliates define who notifies whom, and how fast, after an incident.