Security Vulnerability Report — Squadi / World Sport Action

Date: 23 February 2026 (updated 24 February 2026) **Reporter:** Casey Toll **Severity:** Critical — Children's PII exposure across multiple sports **Status:** Undisclosed (responsible disclosure)

Executive Summary

A hardcoded authentication token embedded in the publicly-accessible NetballConnect JavaScript bundle grants unauthenticated access to personal information of all registered players across all competitions in Australia. This includes **children's full names, dates of birth, parent email addresses, and phone numbers**.

The data is accessible to anyone with a web browser and basic technical knowledge. No account, login, or special tools are required. **A person with no technical training could extract this data in minutes using only a browser's built-in developer tools.**

The same token also grants access to player data on the Squadi basketball platform, indicating the exposure extends beyond netball to all sports managed by Squadi / World Sport Action.

Conservative estimate: 300,000 – 500,000 children's records are exposed, with parent contact details attached to each one. Historical records dating back to at least 2022 remain accessible.

Affected Systems

- **Platform:** Squadi / World Sport Action (trading as NetballConnect, BasketballConnect, and others)
- **APIs confirmed affected:**
  - `api-netball.squadi.com` — All netball competitions nationally
  - `api-basketball.squadi.com` — All basketball competitions nationally
  - `api.squadi.com` — Football/soccer competitions (unified platform)
- **Scope:** All competitions, all organisations, all registered players across all three confirmed Squadi sports platforms
- **Web application:** `registration.netballconnect.com`

How Easy Is This to Exploit?

This vulnerability requires **no hacking, no password cracking, and no special tools**. The steps are:

Step	Difficulty	Time Required
Find team IDs	Trivial — public endpoint, no auth needed	Seconds
Get the auth token	Trivial — visible in the browser's page source (right-click → View Source)	Seconds
Get full rosters with PII	Trivial — one API call per team with the token from the source	Seconds per team
Bulk harvest all players nationally	Low — a simple script enumerating competitions and teams	Minutes to hours

A teenager with browser developer tools could access this data. There is no rate limiting on any endpoint, meaning automated bulk extraction faces no barriers.

Vulnerability Details

1. Hardcoded Authentication Token in Public JavaScript

The NetballConnect web application bundles a default API token directly into its publicly-served JavaScript file:

File: `https://registration.netballconnect.com/static/js/main.010fda61.js`

Token location in source: Search for `REACT_APP_DEFAULT_AUTH_TOKEN`

This token is loaded by every visitor's browser and can be extracted by viewing the page source or browser developer tools (Network tab). It is sent as the `Authorization` header on API requests.

2. Player PII Accessible via Team Roster Endpoint

Using the hardcoded token, the following API call returns full personal information for every player on a team:

```
GET https://api-netball.squadi.com/livescores/teams/id/{teamId}
Authorization: <hardcoded token from JS bundle>
```

Response includes for each player:

- `firstName`, `lastName` — Full name
- `dateOfBirth` — Date of birth (ISO format)
- `email` — Parent/guardian email address
- `phoneNumber` — Parent/guardian phone number
- `userId` — Internal user identifier
- `teamId` — Team assignment
- `competitionId` — Competition assignment

3. Team IDs Are Publicly Enumerable

Team IDs can be obtained without any authentication:

```
GET https://api-netball.squadi.com/livescores/teams?competitionId={id}&organisationId={orgId}
```

This returns all teams in a competition with their IDs, names, and division details. No token required.

4. Competition IDs Are Publicly Enumerable

Competition IDs are sequential integers. The following public endpoint returns competition details:

```
GET https://api-netball.squadi.com/livescores/competitions/id/{competitionId}
```

No authentication required. A simple scan from ID 1 upwards reveals every competition.

5. Cross-Platform Exposure

The same hardcoded token grants access to player PII on all three Squadi sports platforms:

Basketball:

```
GET https://api-basketball.squadi.com/livescores/teams/id/{teamId}
Authorization: <same hardcoded token>
```

Verified against comp 2000 ("2025/26 Club Maitland City Junior Summer Competition") — full player PII returned.

Football/Soccer:

```
GET https://api.squadi.com/livescores/teams/id/{teamId}
Authorization: <same hardcoded token>
```

Verified against comp 98 (Macarthur Football Association) — full player PII returned. Note this uses a different API host (`api.squadi.com` rather than `api-{sport}.squadi.com`), indicating it is a separate/newer deployment, yet the same token grants access.

Attack Chain (Proof of Concept)

An attacker can extract all player PII nationally in four steps:

Step 1 — Enumerate competitions:

```
# Sequential IDs, no auth needed
curl https://api-netball.squadi.com/livescores/competitions/id/4650
# Returns: competition name, unique key, organisation details
```

Step 2 — List all teams in a competition:

```
# No auth needed
curl "https://api-netball.squadi.com/livescores/teams?
competitionId=4650&organisationId=491"
# Returns: 100 teams with IDs, names, divisions
```

Step 3 — Extract the hardcoded token:

```
# View page source or JS bundle
curl https://registration.netballconnect.com/static/js/main.010fda61.js
# Search for: REACT_APP_DEFAULT_AUTH_TOKEN
```

Step 4 — Get full roster with PII for any team:

```
curl -H "Authorization: <token>" \
  "https://api-netball.squadi.com/livescores/teams/id/194366"
# Returns: every player's name, DOB, email, phone
```

No rate limiting was observed on any endpoint.

Potential for Harm

The combination of data exposed enables several harmful scenarios:

- **Targeted contact of minors:** An attacker has children's full names, ages (from DOB), locations (from competition/venue data), and direct contact details for their parents.
- **Convincing phishing attacks:** "Hi [parent name], this is regarding [child name]'s registration for [competition name] at [venue]..." — every detail needed to craft a believable message is available through the API.
- **Bulk data harvesting:** With no rate limiting, a simple script could extract the entire national database of registered players in hours. There is no way to detect or prevent this with the current architecture.
- **Identity fraud:** Dates of birth combined with full names and parent details provide a foundation for identity-related fraud, particularly concerning for minors whose credit histories are typically unmonitored.

How Long Has This Been Exposed?

Evidence from the Internet Archive (Wayback Machine) shows:

Date	Evidence
28 Nov 2023	Earliest archived snapshot of `registration.netballconnect.com`
18 Dec 2023	Earliest archived JS bundle — **already contains the same hardcoded token**
Feb 2026	Current JS bundle — **same token, unchanged after 2+ years**

- The token has been present in **every archived JS bundle version** (26 different builds) across the full 2+ year archive history
- The token has **never been rotated** — the same value appears in Dec 2023 as in Feb 2026
- Player data from competitions labelled "2022" remains accessible, meaning records span **at least 4 years**
- The platform (World Sport Action / Squadi) may predate the NetballConnect branding, extending the exposure window further

The absence of any token rotation in 2+ years suggests there is no monitoring for unauthorised API access and no token management policy.

Verified Impact — Nillumbik Force Netball Association

As a proof of concept, I queried the 10 Hazel Glen Netball Club teams registered in the 2026 NFNA Saturday Autumn competition (competitionId 4650):

Team	Players Exposed
HG 11 Fever	9
HG 11 Fire	9
HG 11 Flames	9

HG 13 Embers	9
HG 13 Fever	8
HG 13 Fury	9
HG 13 Scorchers	9
HG 15 Embers	9
HG 15 Fever	9
HG 15 Flames	10

Total: 90 players' PII from one club alone. The NF competition has 100 teams total (~900 players). The same method works for any competition ID on the platform.

Confirmed exposed data for a specific player (my daughter, verified with parental consent):

- Full name, date of birth (minor — age 13), parent email, parent phone number

---

Scale Estimate

Data Point	Value
Netball player IDs in database	~1,270,000+ (based on sequential ID enumeration)
Basketball player IDs	Additional (separate database, same token)
Football/soccer player IDs	Additional (separate database on `api.squadi.com`, same token)
Competition IDs (netball)	4,750+ competitions spanning 2022–2026
Competition IDs (basketball)	2,000+ competitions
Competition IDs (football/soccer)	100+ competitions
Estimated children's records exposed (netball)	300,000 – 500,000
Total records including adults and all sports	Potentially 1,000,000+
User profile IDs (`/users/public/userProfile`)	~16,000,000 sequential IDs returning names

Note: Many players re-register each season, so unique individuals may be lower than total records. However, historical records (including old email/phone numbers) remain accessible and may still be sensitive.

Additional Public Endpoints of Concern

These endpoints require no authentication and expose additional data:

Endpoint	Data Exposed

`/livescores/competitions/id/{id}`	Competition name, org, venue address, GPS coordinates, phone
`/livescores/teams?competitionId={id}`	All teams, division structure, team IDs
`/livescores/teams/ladder/v2?divisionId={id}&competitionKey={key}`	Full ladder standings
`/livescores/round/matches?competitionKey={key}&divisionId={id}`	Match schedules, scores, venues
`/livescores/matches/periodScores?matchId={id}`	Quarter scores, scorer/manager user IDs
`/users/public/userProfile?userId={id}`	First name, last name (~16M sequential IDs, no rate limit)
`/matches/public/gameSummary?matchId={id}`	Match details with official names
`/stats/public/v2/scoringByPlayer`	Player scoring statistics (where enabled)

Australian Privacy Law Implications

This exposure likely triggers obligations under Australian privacy legislation:

- **Privacy Act 1988:** Organisations handling personal information must take reasonable steps to protect it from misuse, interference, loss, and unauthorised access. A hardcoded token in public JavaScript does not meet this standard.
- **Australian Privacy Principles (APPs):** APP 11 requires reasonable security measures for personal information. APP 6 restricts use and disclosure. The open API effectively discloses all collected data to anyone.
- **Notifiable Data Breaches (NDB) scheme:** Organisations must notify the OAIC and affected individuals when a data breach is likely to result in serious harm. Children's PII (including DOB and parent contact details) being openly accessible for 2+ years likely meets this threshold.
- **Children's data:** The Privacy Act and the Children's Online Privacy guidelines impose heightened obligations when handling minors' personal information.
- **Shared responsibility:** Both Squadi (as data processor/platform provider) and the sporting organisations (as data controllers who collected the information via the platform) may have obligations.

The 30-day assessment period under the NDB scheme begins when the entity becomes aware of the breach.

Recommended Remediation

Immediate (within 24–48 hours)

1. **Remove the hardcoded token** from the JavaScript bundle. Use proper authentication (OAuth/session tokens) that requires user login.
2. **Restrict the `/livescores/teams/id/` endpoint** to require authenticated, authorised access (e.g., only team managers/coaches can see their own team's PII).
3. **Strip PII from public-facing responses** — team listings and rosters should not include email, phone, or DOB unless the requester has a legitimate need and proper authorization.

Short-term (within 1–2 weeks)

4. **Audit all endpoints** returning PII (email, phone, DOB) across all sport platforms and ensure they require proper authorisation.
5. **Implement rate limiting** on all API endpoints to prevent bulk enumeration.
6. **Review server access logs** for any historical bulk access patterns that may indicate prior data harvesting.
7. **Assess NDB notification obligations** — if the breach meets the serious harm threshold, notify the OAIC and affected individuals within the required timeframe.

Medium-term (within 1–3 months)

8. **Review the `/users/public/userProfile` endpoint** which exposes names for ~16 million sequential user IDs with no rate limiting.
9. **Rotate all API tokens** after removing the hardcoded one, as the current token has been publicly cached (including in the Internet Archive) for 2+ years.
10. **Implement proper API authorization architecture** — separate public data (ladders, scores, schedules) from sensitive data (player PII) with different access controls.
11. **Conduct a full security audit** of the platform, including all sport-specific APIs.

Questions for Squadi

The following questions should be raised with Squadi as part of the incident response:

1. Do your server logs show any bulk access or unusual API usage patterns over the past 2+ years?
2. How many sports and organisations use this platform and are affected?
3. The same hardcoded token has been confirmed working across netball, basketball, and football/soccer platforms — are any additional sports affected?
4. Were you aware that the `REACT_APP_DEFAULT_AUTH_TOKEN` was embedded in client-side JavaScript?
5. What is your plan and timeline for remediation?
6. Have you assessed your obligations under the Notifiable Data Breaches scheme?

Recommended Notification Chain

Organisation	Role	Why They Need to Know
Squadi / World Sport Action	Platform provider (data processor)	Must fix the vulnerability and assess NDB obligations
Netball Victoria	State sporting body (data controller)	Regulatory obligations for Victorian player data; manages the relationship with Squadi
Netball Australia	National body	National scope; may need to coordinate across all state/territory bodies
Basketball Australia / state bodies	National/state bodies	Basketball platform confirmed affected with same vulnerability
Football Australia / state bodies	National/state bodies	Football/soccer platform confirmed affected with same vulnerability

OAIC	Regulator	If Squadi does not respond within 30 days, or if they fail to meet NDB obligations

Suggested Netball Victoria Contacts

- **Penny Forrest** — Child Safety & Integrity Coordinator (directly responsible for child safety)
- **Rebecca Costanzo** — Head of Integrity and Compliance (data breach obligations)
- **Rohan Safstrom** — IT Support and Services Manager (technical understanding)
- **Ginny Robinson** — Systems Relationship Manager (likely manages the Squadi relationship)

Disclosure Timeline

Date	Action
23 Feb 2026	Vulnerability discovered during authorised development work
23 Feb 2026	Impact verified using reporter's own child's data (with parental consent)
23 Feb 2026	Cross-platform impact confirmed (basketball and football/soccer APIs)
23 Feb 2026	Historical exposure confirmed via Internet Archive (token present since at least Dec 2023)
23 Feb 2026	Report prepared for responsible disclosure
24 Feb 2026	Report to be sent to Netball Victoria and Squadi
Pending	Vendor acknowledgement
Pending	Fix deployed
90 days	Standard responsible disclosure window before public disclosure

---

Contact

Reporter: Casey Toll **Context:** Parent and coach at Hazel Glen Netball Club. The vulnerability was discovered during routine API exploration for an unofficial personal project that integrates with Squadi's public ladder/fixture APIs. This project is not affiliated with or endorsed by any club, association, or sporting body.

This report is provided in good faith under responsible disclosure principles. No data was extracted beyond what was necessary to verify the vulnerability, and no data has been stored or shared. The reporter has no malicious intent and is willing to assist with remediation efforts.

This report represents the findings of an individual. It is not made on behalf of Hazel Glen Netball Club, Nillumbik Force Netball Association, or any other organisation.