

PDPC and CSA urge firms to lock down APIs, citing Marina Bay Sands and Tech in Asia data breaches

Description

default watermark

Organisations that handle personal data should know every application programming interface (API) that touches it, lock those APIs down and watch how they are used, the Personal Data Protection Commission (PDPC) and the Cyber Security Agency of Singapore (CSA) said in a joint advisory on 12 November 2026.

APIs are the connectors that let a mobile app pull a customerâ??s record from a database, or let a third-party provider reach the data it needs to deliver a service. Attackers can get in through them too, sometimes with valid credentials, so their requests look legitimate and large volumes of personal data can leave without anyone noticing.

The advisory points to two past breaches. At Marina Bay Sands, a misconfigured API endpoint and weak default credentials let a threat actor take the personal data of about 665,495 people. At Tech in Asia, an old endpoint that did not verify authorisation tokens was used to scrape data on about 220,000 people. Section 24 of the Personal Data Protection Act requires organisations to make reasonable security arrangements for personal data in their care.

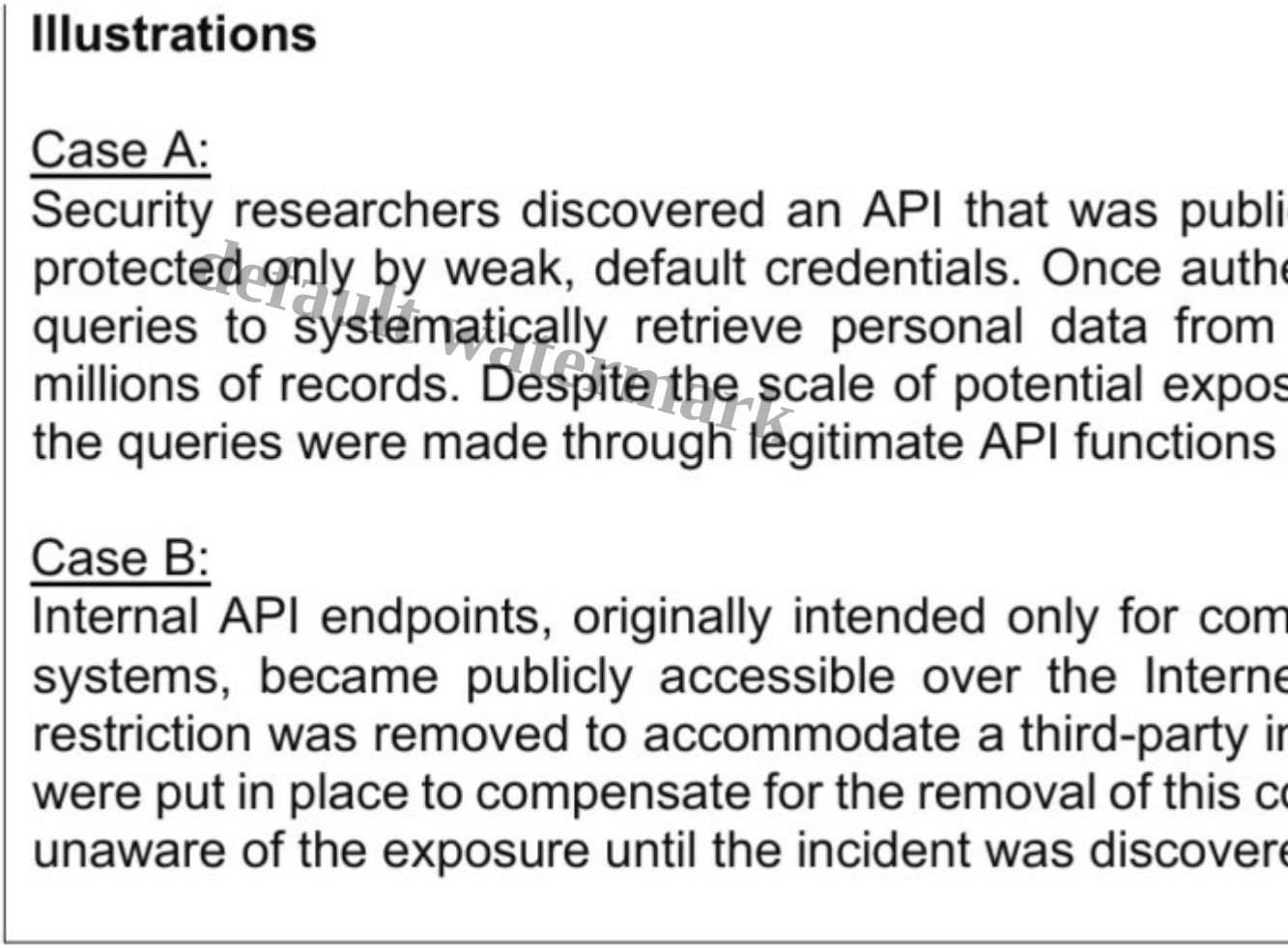
Five ways APIs leak data

The advisory groups the risk into five areas. APIs can expose more data than a request needs, or an internal API can end up reachable from the Internet after a system change. Default or poorly managed credentials, including stolen API keys and access tokens, let outsiders in through legitimate functions. Weak authorisation is the third. The advisoryâ??s example is Broken Object Level Authorisation, ranked first in the OWASP API Security Top 10, where a logged-in customer changes an ID in a request and gets someone elseâ??s record.

The last two are configuration and logging. Security settings can drop out during migrations, unencrypted connections invite man-in-the-middle interception, and unchecked inputs open the door to SQL injection. Without proper logs, an attacker holding valid credentials can keep scraping data

undetected.

Two illustrations show how ordinary the failures are. In one, security researchers found an Internet-facing API protected only by weak, default credentials and pulled personal data from a database of millions of records without being detected. In the other, a network restriction was removed to accommodate a third-party integration, nothing replaced it, and internal endpoints sat exposed until the incident was discovered.



The two case illustrations in the joint advisory. Image: PDPC and CSA

Nine measures, from inventory to incident response

The first measure is knowing what exists: an up-to-date inventory of every API that touches personal data, with its purpose, owner, data types and third-party connections, and obsolete APIs switched off. The second is returning only the fields a request genuinely needs.

On configuration and access, internal APIs should not be reachable from the Internet, every request should be checked against what that user or application is allowed to see, traffic should run over HTTPS with TLS, inputs should be validated on the server with parameterised queries, and a web application firewall should sit in front of Internet-facing APIs. Credentials need strong non-default passwords, multi-factor authentication for privileged access, and API keys kept out of source code and plaintext files, with compromised keys revoked promptly.

The remaining measures cover security reviews before and after any change, especially one that removes a control for a partner integration, plus penetration testing before deployment, periodically and after major changes. Logging should capture who called which function, when, and how much data came back, and higher-risk systems should raise alerts on unusual volumes, even from valid accounts. Rate limits and caps on data per request reduce the damage, and incident plans should cover revoking credentials, suspending access and deciding whether affected individuals or the PDPC need to be notified under the Act.

The advisory builds on the PDPCâ??s Guide to Data Protection Practices for ICT Systems, revised on 20 July 2026. It points organisations to CSAâ??s Technical Advisory on Secure API Development for detailed technical guidance, and says SMEs may want to look at government assistance schemes for cybersecurity. Businesses hit by an incident can also call the Cyber Incident Helpline on 6890 9555. The full joint advisory is on CSAâ??s website.

default watermark

Date Created
13/11/2026
Author
vanessakoh