New guidance on securing HTTP-based APIs

Why it's essential to secure your APIs to build trust with your customers and partners.

James H

From social media platforms to the financial sector, to healthcare and telecoms. APIs (application programming interfaces) underpin a vast range of digital functions, and facilitate seamless data exchange between systems and services.

Unfortunately, this increasing use of APIs provides attackers with greater opportunities to exploit vulnerabilities within their design and implementation.

Recent public reports on high-profile API security breaches include:

- attackers exploiting insufficient authentication and a lack of rate limiting in Dell's Partner Portal API to steal the personal details of 49 million customers
- in a separate incident, a misconfigured and poorly-secured Trello API led to the exposure of personal data for over 15 million users
- the automotive industry faced a similar threat when an API vulnerability in Kia's Web Portal allowed hackers to remotely track, unlock, and start customers' vehicles
- and in telecommunications, the Optus data breach was caused by a forgotten, poorly secured API that remained online for years

In response to this increased threat, the NCSC has published new guidance on securing HTTP-based APIs, which is designed to help technical staff to design or build secure applications that offer an HTTP API.

Relying on outdated security methods (such as basic authentication using base64-encoded usernames and passwords) is no longer sufficient. Other bad practices that the guidance addresses includes:

- the absence of rate limiting or user throttling
- leaving endpoints vulnerable to denial of service or brute-force attacks
- storing credentials in code

- transmitting sensitive data in URLs
- poor input validation
- failing to encrypt API traffic using HTTPS
- minimising unnecessary exposure to the internet
- neglecting proper logging and monitoring

Historically, API keys have been a popular choice for authenticating and authorising API requests, acting as shared credentials between clients and servers. But they come with significant security risks:

1. They are prone to theft through methods like phishing, exposure in leaked source code or improper storage.
2. The absence of built-in expiration means that if a key is compromised it can be exploited indefinitely (unless manually revoked or rotated).
3. API keys fail to provide granular control, often enabling unrestricted access instead of tailored permissions (which combined with an absence of rate limiting can allow attackers swift and unrestricted access to sensitive data).

For all these reasons, relying solely on API keys is no longer considered best practice, which is why the guidance includes information about stronger authentication frameworks such as OAuth 2.0 or token-based authentication.

As the above examples illustrate, the impact of your API being compromised could disrupt operations, damage your organisation's reputation and may even lead to fines from regulatory bodies. Strengthening API security should not simply be seen as a protective measure; it can also enable organisations to enhance agility, simplicity and productivity.

We hope that you use the new guidance to secure your APIs and build trust with your customers and partners, whilst mitigating the risk of financial or reputational damage.

James H
Telecoms Security Consultant

PUBLISHED

/

WRITTEN BY

James H
Telecoms Security Consultant

3 April 2025

WRITTEN FOR

Cyber security professionals

PART OF BLOG

NCSC publications