



GeoVision Security Advisory

Release Date: 2026/09/30

Advisory ID:

GV-Eye-2026-09-01

CVE ID:

CVE-2026-103096, CVE-2026-103097, CVE-2026-103098

Affected Product:

GV-Eye V3.6.0 Android or earlier

Security Issue:

CVE-2026-103096, CVE-2026-103097

An API key is hardcoded and retrievable from the application package. Since Android applications can be reverse engineered, embedding sensitive API credentials directly in the client application may allow unauthorized users to extract and misuse the key.

CVE-2026-103098

Transmission of a sensitive key in the URL over an unencrypted HTTP connection. The request is sent over HTTP rather than HTTPS, meaning the key is transmitted in plaintext across the network. An attacker with the ability to monitor network traffic could intercept the request and obtain the key.

Resolution:

Reported vulnerabilities have been resolved with App update V3.7.2. User may contact GeoVision Support team at support@geovision.com.tw to request for the update file or download the V3.7.2 from GeoVision's Google play.

If you have any questions or concerns in regards the cybersecurity issue, please contact our cybersecurity team: security@geovision.com.tw.