GeoVision Security Advisory

Release Date: 2026/09/10

Advisory ID:

GV-LPC-2026-09-01

CVE ID:

CVE-2026-88268, CVE-2026-88269, CVE-2026-88270, CVE-2026-88271, CVE-2026-88272, CVE-2026-88273, CVE-2026-88274, CVE-2026-88275, CVE-2026-88276, CVE-2026-88277, CVE-2026-88278, CVE-2026-88279, CVE-2026-88280, CVE-2026-88281, CVE-2026-88282, CVE-2026-88283, CVE-2026-88284, CVE-2026-88285, CVE-2026-88286, CVE-2026-88287, CVE-2026-88288, CVE-2026-88289, CVE-2026-88290

Affected Product:

GV-LPC2011/LPC2211 V1.13 or earlier

GV-LPC2011/LPC2211 V1.14 20260903 Pre-Test version

Security Issue:

CVE-2026-88268

An authenticated stack-based buffer overflow in SSVR fragment reassembly allows a valid user to crash the SSVR service.

CVE-2026-88269

A Guest user can retrieve persistent device configuration containing plaintext administrative and user credentials through SSVR.

CVE-2026-88270

A Guest user can enter SSVR firmware-upgrade mode and disrupt live services before any firmware image is validated.

CVE-2026-88271

A Guest user can overwrite device configuration and replace the administrator password through SSVR.

CVE-2026-88272

An administrator-controlled username containing shell metacharacters can be executed as arbitrary root commands when the stored username is later deleted.

CVE-2026-88273

An administrator-controlled PPPoE username can escape a sourced shell configuration assignment and execute arbitrary commands as root.

CVE-2026-88274

An administrator-controlled wireless SSID containing shell syntax can execute arbitrary commands as root.

CVE-2026-88275

An administrator-controlled WPA-PSK containing shell syntax can execute arbitrary commands as root when wireless configuration is applied.

CVE-2026-88276

Administrator-controlled WEP key values containing shell syntax can be used to execute arbitrary commands as root.

CVE-2026-88277

An authenticated ONVIF user can inject shell commands through ConsumerReference.Address and execute arbitrary commands as root.

CVE-2026-88278

The device fails to enforce WS-Security UsernameToken freshness or nonce-reuse protection, allowing a captured PasswordDigest token to be replayed for subsequent ONVIF operations.

CVE-2026-88279

Oversized ONVIF CreateUsers username or password values are copied into fixed-size stack fields, allowing an authenticated administrator to crash the ONVIF worker.

CVE-2026-88280

An oversized ONVIF SetUser password can be copied into a fixed-size stack field, allowing an authenticated administrator to crash the ONVIF worker.

CVE-2026-88281

The device fails to limit repeated Username elements in ONVIF DeleteUsers requests, allowing an authenticated administrator to overflow a stack array and crash the ONVIF worker.

CVE-2026-88282

An administrator-controlled FTP username containing shell metacharacters can be executed as arbitrary root commands during a subsequent FTP-account update.

CVE-2026-88283

The device fails to limit repeated User elements in ONVIF CreateUsers requests, allowing an authenticated administrator to overwrite stack control state and crash the ONVIF worker.

CVE-2026-88284

The device fails to limit repeated User elements in ONVIF SetUser requests, allowing an authenticated administrator to overwrite stack control state and crash the ONVIF worker.

CVE-2026-88285

A network-accessible PTZ control service is exposed without authentication, allowing remote clients to retrieve PTZ information and issue PTZ or raw serial commands.

CVE-2026-88286

Improper PTZ connection-state management allows an unauthenticated remote client to block the accept loop and prevent new PTZ connections.

CVE-2026-88287

The device fails to bound the number of Scopes tokens in unauthenticated ONVIF WS-Discovery Probe requests, allowing a remote attacker to corrupt stack control state and crash the discovery process.

CVE-2026-88288

The device fails to restrict the filename supplied to BKDownloadLink.cgi, allowing a remote user with valid web credentials to read arbitrary files accessible to the root-run web service.

CVE-2026-88289

Multiple VLSVR request handlers fail to validate attacker-controlled variable-length fields before copying them into fixed-size stack buffers, allowing an unauthenticated remote attacker to crash the VLSVR service.

CVE-2026-88290

Unauthenticated clients can declare unbounded VLSVR frame lengths and indefinitely delay blocking receives, potentially exhausting memory, connections, and worker resources.

Resolution:

Reported vulnerabilities are resolved with firmware update GV-LPC2011/2211 V1.14 and later official release versions. User may use GeoVision's download page to download the firmware update or contact GeoVision Support at support@geovision.com.tw for further assistance.

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