GeoVision Security Advisory

Release Date: 2026/06/26

Advisory ID:

GV-LPC-2026-06-01

CVE ID:

CVE-2026-57872, CVE-2026-57873, CVE-2026-57874, CVE-2026-57875, CVE-2026-57876, CVE-2026-57877, CVE-2026-57878, CVE-2026-57879, CVE-2026-57880, CVE-2026-57881

Affected Product:

GV-LPC2011/LPC2211 V1.12 or earlier

Security Issue:

CVE-2026-57872

An unauthenticated directory traversal vulnerability exists in get_fcont.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient validation of user-supplied file path input before the requested file is accessed by the CGI component. A remote attacker may exploit this vulnerability by sending a crafted request to read arbitrary files accessible to the affected process, resulting in information disclosure.

CVE-2026-57873

An unauthenticated NULL pointer dereference vulnerability exists in IEEE8021x_upload.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper validation of multipart upload headers when processing certificate-related upload fields. A remote attacker may exploit this vulnerability by sending a malformed multipart request, causing the affected CGI process to crash and resulting in a denial of service.

CVE-2026-57874

An unauthenticated buffer overflow vulnerability exists in IEEE8021x_upload.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when parsing filename values in multipart upload data. A remote attacker may exploit this vulnerability by sending a crafted upload request with overly long input, causing memory corruption and resulting in a denial of service.

CVE-2026-57875

An unauthenticated NULL pointer dereference vulnerability exists in the HTTP request parsing logic of multiple CGI components in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper validation of required HTTP request metadata before it is used by the affected components. A remote attacker may exploit this vulnerability by sending a specially crafted HTTP request, causing the affected process to crash and resulting in a denial of service.

CVE-2026-57876

An unauthenticated out-of-bounds write vulnerability exists in onvif.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing HTTP request body data. A remote attacker may exploit this vulnerability by sending a crafted request with excessive input, causing memory corruption and resulting in a denial of service.

CVE-2026-57877

An unauthenticated format string vulnerability exists in vlsvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper handling of externally controlled input during log message formatting in the login processing path. A remote attacker may exploit this vulnerability by sending crafted login data, potentially causing information disclosure, memory corruption, or a denial of service.

CVE-2026-57878

An unauthenticated stack-based buffer overflow vulnerability exists in thttpd in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing web request parameters in a specific request path. A remote attacker may exploit this vulnerability by sending a crafted HTTP request with overly long input, resulting in memory corruption, denial of service, or potentially arbitrary code execution.

CVE-2026-57879

An unauthenticated stack-based buffer overflow vulnerability exists in ssvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing RTSP custom authentication data. A remote attacker may exploit this vulnerability by sending a crafted RTSP request, resulting in memory corruption, denial of service, or potentially arbitrary code execution.

CVE-2026-57880

An unauthenticated stack-based buffer overflow vulnerability exists in ssvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when parsing RTSP Digest authentication fields. A remote attacker may exploit this vulnerability by sending a crafted RTSP request containing overly long authentication data, resulting in memory corruption, denial of service, or potentially arbitrary code execution.

CVE-2026-57881

An unauthenticated stack-based buffer overflow vulnerability exists in vlsvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient length validation when processing remote login data. A remote attacker may exploit this vulnerability by sending crafted login data with overly long input, resulting in memory corruption, denial of service, or potentially arbitrary code execution.

Resolution:

Reported vulnerabilities are resolved with firmware update GV-LPC2011/2211 V1.13 and later 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.