GeoVision Security Advisory

Release Date: 2026/06/17

Advisory ID:

GV-IOBOX-2026-06-01

CVE ID:

CVE-2026-12485, CVE-2026-12846, CVE-2026-12847, CVE-2026-12848,
CVE-2026-12486, CVE-2026-12849, CVE-2026-12850, CVE-2026-12851

Affected Product:

GV-I/O BOX Series V2.0.9 or earlier

Security Issue:

CVE-2026-12485, CVE-2026-12846, CVE-2026-12847, CVE-2026-12848,

A buffer overflow vulnerability exists in the DVRSearch CMD_IP_SET functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network request can lead to a arbitrary code execution. An attacker can send a network request to trigger this vulnerability.

CVE-2026-12486, CVE-2026-12849, CVE-2026-12850, CVE-2026-12851

Multiple OS command injection vulnerabilities exist in the libNetSetObj.so functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network packet can lead to command execution. An attacker can send a network request to trigger this vulnerability.

Resolution:

Reported vulnerabilities are resolved with firmware update GV-I/O Box V2.12. User may visit our download page https://www.geovision.com.tw/download/product/ or contact GeoVision Support at support@geovision.com.tw for assistance

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