GeoVision Security Advisory

Release Date: 2026/06/24

Advisory ID:

GV-GeoWebPlayer-2026-06-01

CVE ID:

CVE-2026-13125, CVE-2026-13131, CVE-2026-13132, CVE-2026-57264, CVE-2026-57265, CVE-2026-57266, CVE-2026-57267, CVE-2026-57268, CVE-2026-57269, CVE-2026-57270, CVE-2026-57271, CVE-2026-57272, CVE-2026-57273, CVE-2026-57274, CVE-2026-57275, CVE-2026-57276, CVE-2026-57277, CVE-2026-57278,

Affected Product:

GV-GeoWebPlayer V1.1.1.0 or earlier

Security Issue:

CVE-2026-13125

A lack of authentication vulnerability exists in the Websocket Server functionality of GeoVision GeoWebPlayer 1.1.1.0. A specially crafted websocket connection can lead to execution of a privileged operation. An attacker can stage a malicious web page to trigger this vulnerability.

CVE-2026-13131, CVE-2026-13132, CVE-2026-57264, CVE-2026-57265, CVE-2026-57266, CVE-2026-57267, CVE-2026-57268, CVE-2026-57269, CVE-2026-57270, CVE-2026-57271, CVE-2026-57272

Multiple out-of-bounds read vulnerabilities exist in the Websocket Server functionality of GeoVision GeoWebPlayer 1.1.1.0. A specially crafted websocket message can lead to arbitrary code execution. An attacker can stage a malicious web page to trigger this vulnerability.

CVE-2026-57273, CVE-2026-57274, CVE-2026-57275, CVE-2026-57276, CVE-2026-57277, CVE-2026-57278,

Multiple stack-based buffer overflow vulnerabilities exist in the Websocket Server connectInfo handler functionality of GeoVision GeoWebPlayer 1.1.1.0. A specially crafted websocket message can lead to an arbitrary code execution. An attacker can stage a malicious webpage to trigger this vulnerability.

Resolution:

Reported vulnerabilities are resolved with software version V1.1.3.0 packaged in GV-VMS V20.1.0.0. User may visit our download page at https://www.geovision.com.tw/download/product/ 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.