Security Advisory: XMRig Attack Vulnerability Response

Article ID: GV0-26-11-12

Release Date: Nov. 12, 2026

Advisory ID: GV-SFW-2026-11-01
Status: Continuously Updated

Affected Products:
GV-VMS V20.0.2 and earlier
GV-VMS V18.3.5
GV-VMS V17.4.8

GeoVision is aware of recent cryptocurrency-mining malware attacks targeting the GeoVision video management system (GV-VMS). **This vulnerability is only exposed when the system is connected to the internet with the WebCam Server feature enabled.** When compromised, Windows servers running GV-VMS have been observed experiencing unexplained, heavy CPU load indicative of XMRig mining.

We urgently request that our GV-VMS users update their systems immediately to the latest version or apply the following patches to enhance WebCam Server cybersecurity:

- **GV-VMS V20:** Update to the latest version V20.1.3
- **GV-VMS V18:** Apply the patch (V18.3.5.25) to VMS version V18.3.5
- **GV-VMS V17:** Apply the patch (V17.4.8.65) to VMS version V17.4.8

If your system has been compromised by the malware, please follow the Malware Removal Guide in the Security Advisory document to clean the infection and resolve the vulnerability.

We encourage our customers to keep their products updated to the latest versions. We will continue to monitor the situation and keep you informed of further developments if anything changes.

If you have further questions, please feel free to contact us: security@geovision.com.tw.