Security Advisory: XMRig attack Vulnerability Response.

Release Date: 2026/11/11

Advisory ID:

GV-SFW-2026-11-01

1. Threat Summary & Initial Attack Vector

Multiple active attacks have been reported targeting internet-exposed GeoVision NVR systems running GV-VMS with Webcam server enabled. Exploitation of unauthenticated Remote Code Execution (RCE) vulnerabilities within the GeoVision WebCam Server while enabled, allows unauthorized attackers to execute arbitrary PowerShell commands under the Windows SYSTEM account, leading to the deployment of XMRig cryptocurrency miners and persistence mechanisms.

Threat Symptons:

Category	Observable symptoms
High CPU usage	Unusually high CPU utilization, including when the server is otherwise idle.
System performance	Slow response, increased CPU temperature, or abnormal fan activity.
Microsoft Defender	Defender processes unexpectedly terminate, fail to start, or show abnormal protection status.
PowerShell activity	Suspicious PowerShell execution involving DownloadString, IEX, encoded commands, or remote script retrieval.
Unknown executables	Unexpected executables such as update.exe or ApplyUpdate.exe in temporary or application directories.
Scheduled tasks	Unknown boot-triggered tasks launching scripts or executables under SYSTEM privileges.
Kernel drivers	Unexpected drivers, including the reported kvckiller.sys and WinRing0x64.sys.
Registry modifications	Unauthorized IFEO Debugger values targeting Defender-related executables.
Network activity	Unexpected outbound connections to mining pools or suspicious external destinations.
Persistence	Miner or malicious processes automatically restart after reboot.

2. Immediate Containment & Isolation Steps

• Disconnect Host from Internet: Immediately unplug the network cable or sever WAN routing to terminate command & Control (C2) communication (e.g., target IP 45.32.117.34, 2.59.133.151, 156.246.94.183).

• Isolate NVR Network Access: Place affected hosts behind a strict firewall/VPN.

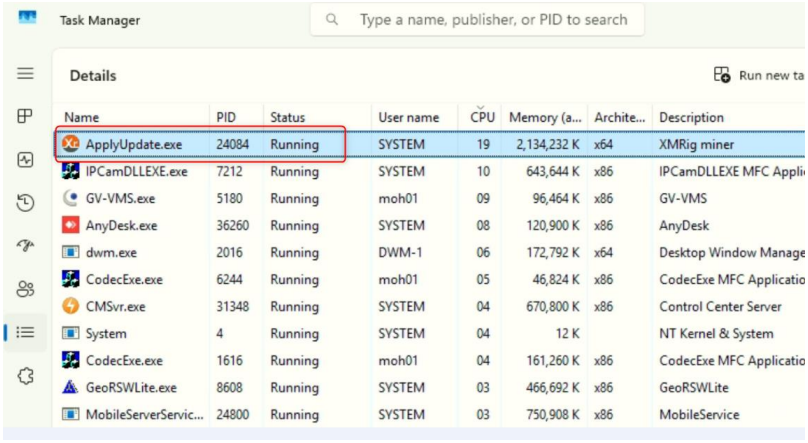
• Restrict Inbound Ports: Immediately block or restrict internet access to standard listening ports such as Port 80, 554, 4550, 5550, 5552, 15552, 3388, 5611, 6550, 6200, 48000.

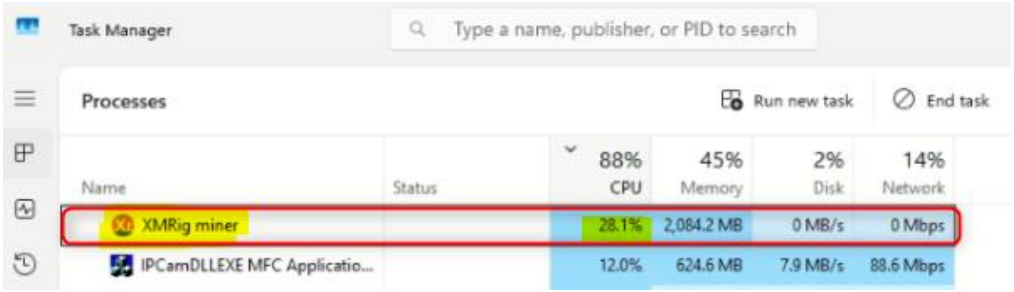
3. Malware removal guide (what to find and delete)

3.1 Terminate Malicious Processes:

Open Task Manager or an elevated PowerShell prompt and end the following process names if found:

- ApplyUpdate.exe (XMRig miner)
- XMRig Minder
- update.exe
- a.exe



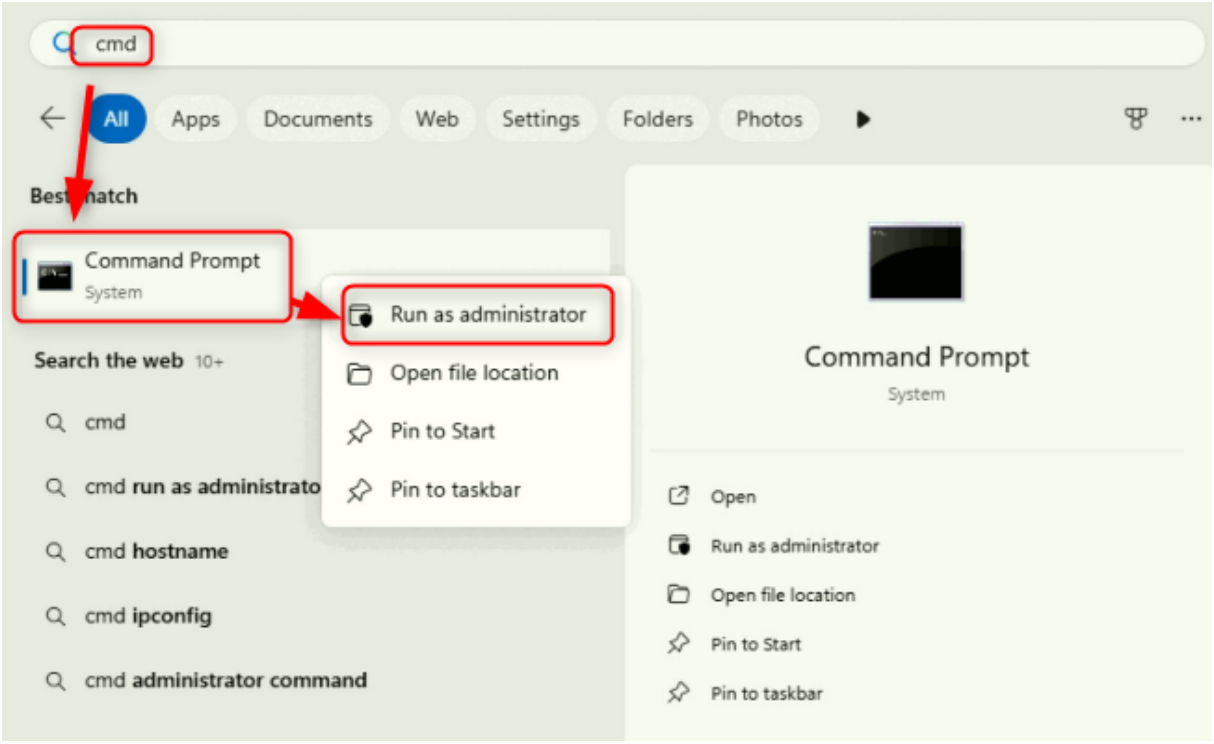


3.2 Search & Delete Malicious Files Locations:

Below are some sample locations and Malicious Files generally located in default GV-VMS camera database location. It is recommended to use Windows file explorer to search and permanently delete the following files from the affected system:

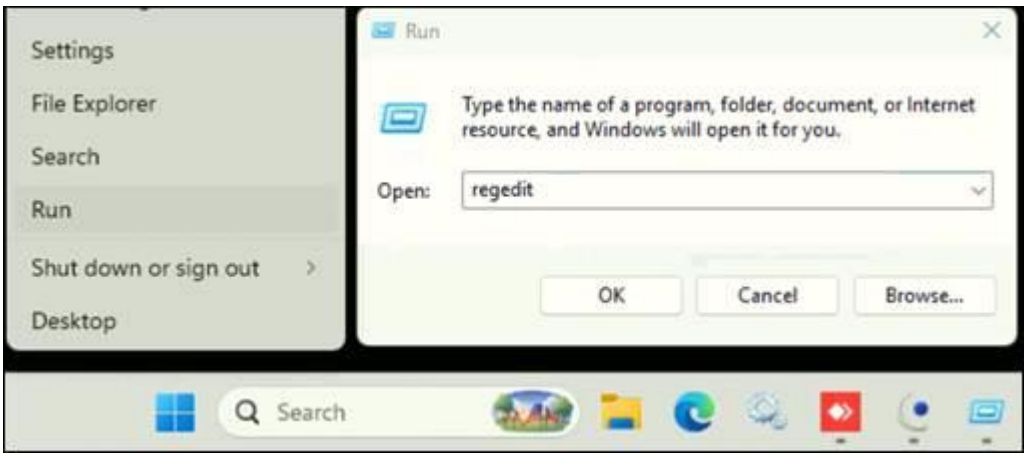
- D:\CameraDBs\b.ps1
- D:\CameraDBs\k.sys
- D:\CameraDBs update.exe
- D:\CameraDBs\PackageUpdater.bat
- C:\Windows\Temp\ApplyUpdate.exe
- C:\Windows\Temp\UpdateData.json
- C:\Windows\Temp\WinRing0x64.sys
- C:\Windows\System32\config\systemprofile\update.exe

3.3 Remove Persistence & Driver Hijacks using elevated command prompt or powershell:

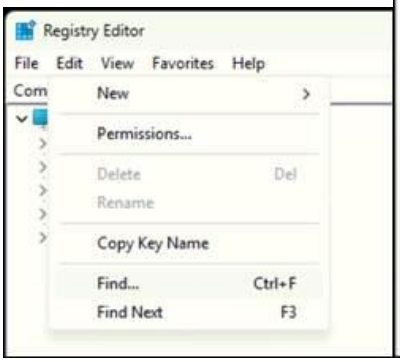


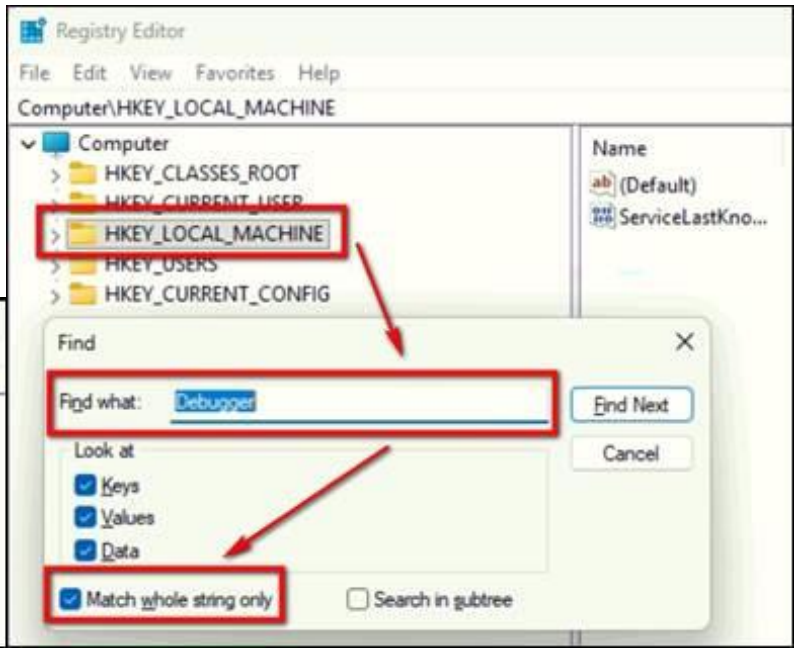
Mechanism Target	Removal Command / Procedure
Scheduled Task	schtasks /delete /tn "PackageUpdater_Startup" /f
Registry Startup Key	reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "PackageUpdater" /f
Malicious Service (wsftprm)	sc stop wsftprm ; sc delete wsftprm
Malicious Service (WinRing0)	sc stop WinRing0_1_2_0 ; sc delete WinRing0_1_2_0
IFEO Hijacks (Defender)	Delete "Debugger" string under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MsMpEng.exe HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SecurityHealthService.exe HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SecurityHealthSystray.exe

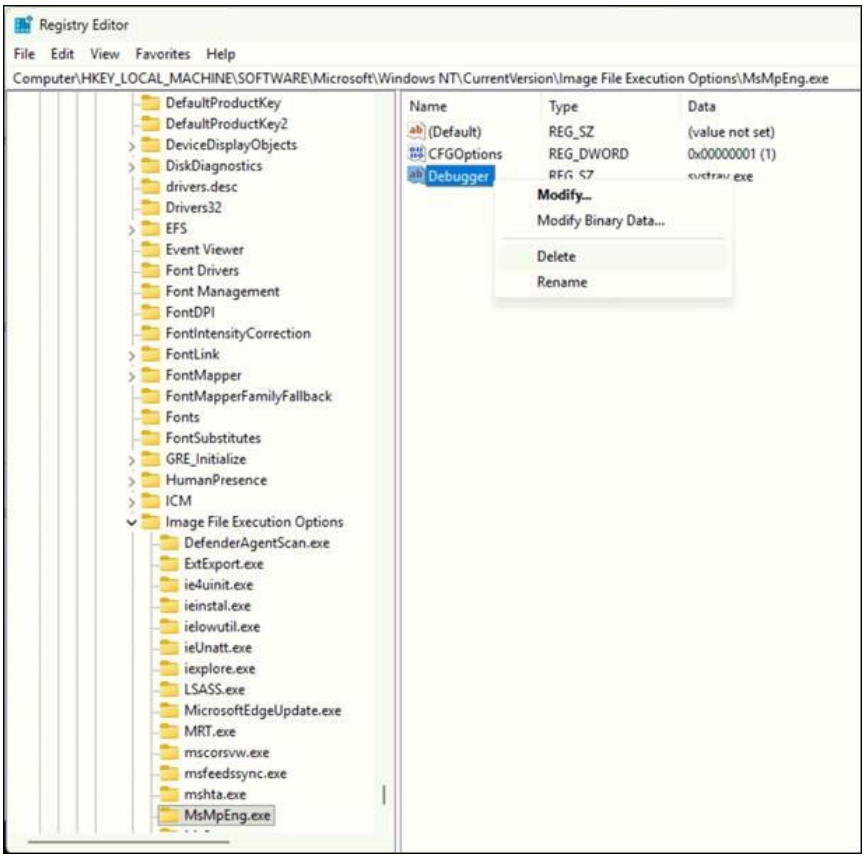
1. Launch Windows Registry editor



2. First, select `HKEY_LOCAL_MACHINE` (this is faster), then click "Find..." (or press `Ctrl+F`) and search for "Debugger." ***Make sure to tick Match whole string only***. You can press the `F3` key to jump directly to the next search result. Locate the three paths you mentioned and delete all instances of "Debugger" found there.



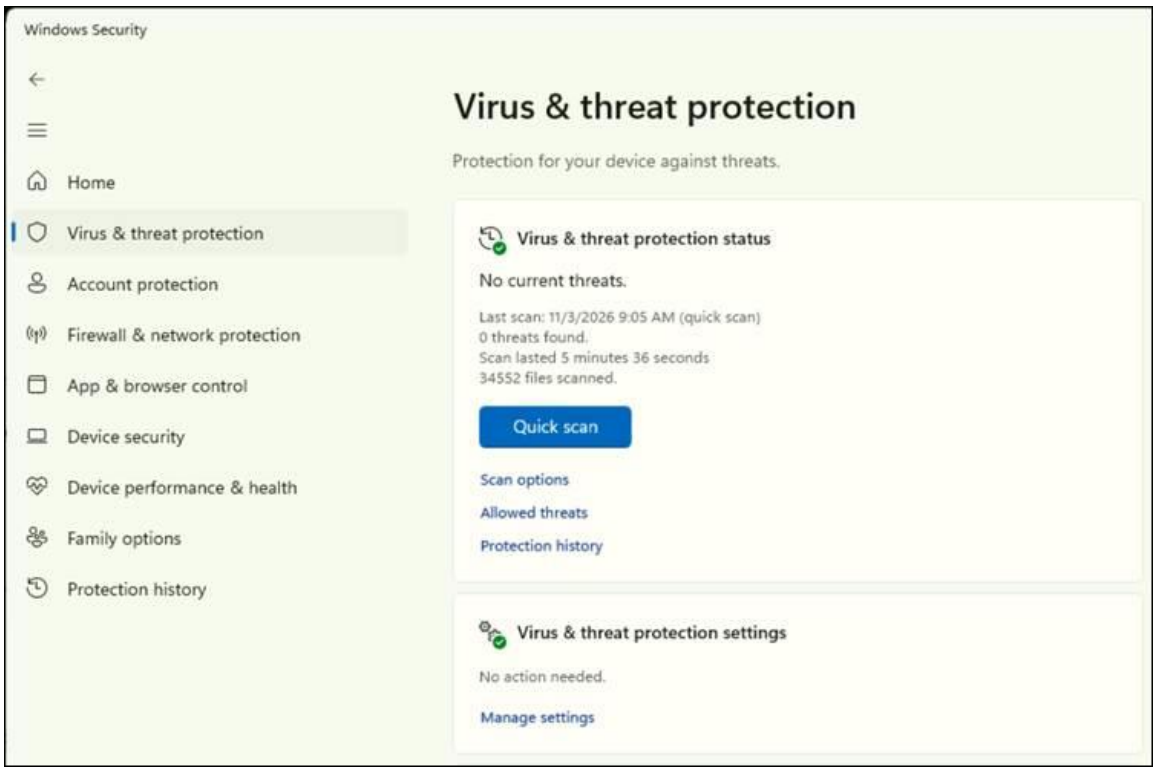




After performing the listed tasks. Go to "Windows Security" (under "Virus & threat protection") and click "Restart now." (It is recommended to restart your PC once you have finished these steps.)



Re-open "Windows Security" (under "Virus & threat protection"); if you see the screen shown in the image below, the process was successful.



4. Forensics & Verification (What more to Check)

• Windows Defender Status: Ensure Defender / EDR services (WinDefend, SecurityHealthService) are active and run a full system scan (Start-MpWDScan).

• Network Sockets: Run “netstat –ano” (without quotes) using command prompt to confirm no active outbound connections exist to C2 IPs 45.32.117.34 or 156.246.94.183.

• Local User Accounts: Verify “net user” (without quotes) using command prompt and to ensure no unauthorized administrative backdoor accounts were created during SYSTEM access.

• PowerShell Logs: Review Event ID 4104 (ScriptBlock Logging) in Microsoft Windows PowerShell/Operational to verify execution history.

• Process Creation Logs: Inspect Security Event ID 4688 to confirm if powershell.exe was spawned directly by GeoVision processes.

5. Permanent Resolution & Patch update

To permanently eliminate the RCE vulnerability, apply the latest GeoVision software releases and patch containing cumulative security fixes for CVE-2026-7372, CVE-2026-42369, and CVE-2026-42370.

V20 -> V20.1.3 Release

Improved:

Cybersecurity enhanced in GV-WebCam Server (Patch V20.0.2.10)

GV-VMS V20 Download page

https://www.geovision.com.tw/download/product/GV-VMS%20V20

GV-VMS V20 Version history

https://dlcdn.geovision.com.tw/Manual/VMS/EN/V20/Version_History_VMS_V20.pdf

V17.4.8 -> V17.4.8.65

Improved:

Cybersecurity enhanced in the WebCam Server. (V17.4.8.58)

V17.4.8 Patch file download page

https://php.gvdip.com/phpbb3/viewtopic.php?t=2638

V18.3.5 -> V18.3.5.25

Improved:

Cybersecurity enhanced in the WebCam Server. (V18.3.5.22)

https://php.gvdip.com/phpbb3/viewtopic.php?t=2651

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