GeoVision Security Advisory

Release Date: Nov 20, 2024

Advisory ID

GV-IP-2024-11-1

CVE ID

CVE-2024-6047

CVE-2024-11120

Affected Product

CVE-2024-6047

DSP LPR	IP Camera	Video Server：	DVR
GV_DSP_LPR_V2	GV_IPCAMD_GV_BX130 GV_IPCAMD_GV_BX1500 GV_IPCAMD_GV_CB220 GV_IPCAMD_GV_EBL1100 GV_IPCAMD_GV_EFD1100 GV_IPCAMD_GV_FD2410 GV_IPCAMD_GV_FD3400 GV_IPCAMD_GV_FE3401 GV_IPCAMD_GV_FE420	GV_GM8186_VS14 GV-VS14_VS14 GV_VS03 GV_VS2410 GV_VS28XX GV_VS216XX GV VS04A GV VS04H	GVLX 4 V2 GVLX 4 V3

CVE-2024-11120

DSP LPR	Video Server：	DVR
GV_DSP_LPR_V3	GV-VS12 GV-VS11	GVLX 4 V2 GVLX 4 V3

Security Issue

Certain EOL GeoVision devices have an OS Command Injection vulnerability due to improper filtering of user input for specific functionalities. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbitrary system commands on the device.

Resolution

The affected devices are no longer maintained and have reached their end of life (EOL). It is recommended that users replace these devices with those currently offered by GeoVision to avoid potential vulnerabilities.

If you have any questions or concerns regarding the reported vulnerability, please contact our cybersecurity team at: security@geovision.com.tw.

奇偶科技安全性通告

編輯日期: Nov 20, 2024

通告 ID

GV-IP-2024-11-1

CVE ID

CVE-2024-6047

CVE-2024-11120

受影響產品

CVE-2024-6047

DSP LPR	IP Camera	Video Server：	DVR
GV_DSP_LPR_V2	GV_IPCAMD_GV_BX130 GV_IPCAMD_GV_BX1500 GV_IPCAMD_GV_CB220 GV_IPCAMD_GV_EBL1100 GV_IPCAMD_GV_EFD1100 GV_IPCAMD_GV_FD2410 GV_IPCAMD_GV_FD3400 GV_IPCAMD_GV_FE3401 GV_IPCAMD_GV_FE420	GV_GM8186_VS14 GV-VS14_VS14 GV_VS03 GV_VS2410 GV_VS28XX GV_VS216XX GV VS04A GV VS04H	GVLX 4 V2 GVLX 4 V3

CVE-2024-11120

DSP LPR	Video Server：	DVR
GV_DSP_LPR_V3	GV-VS12 GV-VS11	GVLX 4 V2 GVLX 4 V3

安全問題

某些已達生命週期（EOL）的 GeoVision 設備存在 OS Command Injection 漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞注入系統指令並於設備上執行。另外，我們已收到相關報告顯示該漏洞已遭利用。

解決方法

該產品已不再維護，建議汰換設備

如果您對報告的漏洞有任何疑問或疑慮，請聯絡我們的網路安全團隊：
security@geovision.com.tw。