Date□2025/05/14

□Vulnerability Alert□CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/05/05-2025/05/11)

- Subject Description: □Vulnerability Alert□CISA Adds 4 Known Exploited Vulnerabilities to KEV Catalog (2025/05/05-2025/05/11)
- Content Description:
    - Forwarded by Taiwan Computer Network Crisis Handling and Coordination Center TWCERTCC-200-202505-00000008
    1. □CVE-2025-3248□Langflow Missing Authentication Vulnerability (CVSS v3.1: 9.8)
       □Ransomware Exploitation: Unknown□ Langflow has an authentication missing vulnerability at the /api/v1/validate/code endpoint, allowing remote unauthenticated attackers to execute arbitrary code through crafted HTTP requests.
       □Affected Platform□ langflow version 1.2.0 (inclusive) and earlier
    2. □CVE-2025-27363□FreeType Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.1)
       □Ransomware Exploitation: Unknown□ FreeType has an out-of-bounds write vulnerability when attempting to parse subfont structures related to TrueType GX and variable font files, which may lead to arbitrary code execution.
       □Affected Platform□ FreeType version 2.13.0 (inclusive) and earlier
    3. □CVE-2024-11120□GeoVision Devices OS Command Injection Vulnerability (CVSS v3.1: 9.8)
       □Ransomware Exploitation: Unknown□ Multiple GeoVision devices have an OS command injection vulnerability, allowing remote unauthenticated attackers to inject and execute arbitrary system commands.
       □Affected Platform□ GV-VS12 GV-VS11 GV-DSP_LPR_V3 GVLX 4 V2 GVLX 4 V3
    4. □CVE-2024-6047□GeoVision Devices OS Command Injection Vulnerability (CVSS v3.1: 9.8)
       □Ransomware Exploitation: Unknown□ Multiple GeoVision devices have an OS command injection vulnerability, allowing remote unauthenticated attackers to inject and execute arbitrary system commands.
       □Affected Platform□ 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
- Affected Platform:
    - Detailed content in the affected platform section of the content description
- Recommended Measures:
    1. □CVE-2025-3248□ Upgrade the corresponding product to the following version (or higher) langflow 1.3.0
    2. □CVE-2025-27363□ Upgrade the corresponding product to the following version (or higher) FreeType 2.13.1
    3. □CVE-2024-11120□ The affected products may have reached end-of-life (EoL) or end-of-service (EoS). It is recommended that users stop using the related products.
    4. □CVE-2024-6047□ The affected products may have reached end-of-life (EoL) or end-of-service (EoS). It is recommended that users stop using the related products.

Network System Division
Computer and Communication Center9

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250514_04

Last update: **2025/05/14 16:12**