Date Posted: 2025/06/30

□Vulnerability Alert□2 Critical Security Vulnerabilities in Hunter Electronic Hybrid Surveillance System Host

- Subject: □Vulnerability Alert□2 Critical Security Vulnerabilities in Hunter Electronic Hybrid Surveillance System Host
- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202506-00000017
  - □Hunter Electronic Hybrid Surveillance System Host - Exposure of Sensitive System Information□(CVE-2025-6561, CVSS: 9.8) Some Hunter Electronic Hybrid Surveillance System Host models (HBF-09KD and HBF-16NK) have an Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to directly access system configuration files and obtain plaintext administrator usernames and passwords.
  - □Hunter Electronic Hybrid Surveillance System Host - OS Command Injection□(CVE-2025-6562, CVSS: 8.8) Some Hunter Electronic Hybrid Surveillance System Host models (HBF-09KD and HBF-16NK) have an OS Command Injection vulnerability, allowing authenticated remote attackers with general privileges to inject arbitrary operating system commands and execute them on the device.
- Affected Platforms:
  - HBF-09KD, HBF-16NK
  - V3.1.67_1786 BB11115 (and earlier versions)
- Suggested Measures:
  - Update firmware version to V31.70_1806 BB50604 (and later versions)
- References:
  1. Hunter Electronic Hybrid Surveillance System Host - Exposure of Sensitive System Information
     - https://www.twcert.org.tw/tw/cp-132-10199-9c5c6-1.html
  2. Hunter Electronic Hybrid Surveillance System Host - OS Command Injection
     - https://www.twcert.org.tw/tw/cp-132-10201-044e9-1.html

---

Computer and Communications Center
Network Systems Division Respectfully

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250630_01

Last update: **2025/06/30 09:18**