POSTING DATE: 2025/12/23

[VULNERABILITY ALERT] WatchGuard Firebox Contains a Critical Security Vulnerability (CVE-2025-14733)

- Subject: [VULNERABILITY ALERT] WatchGuard Firebox Contains a Critical Security Vulnerability (CVE-2025-14733)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000010
  - WatchGuard Firebox is a next-generation firewall product that provides multi-layered protection, including antivirus, IPS, APT blocking, and spam filtering.
  - WatchGuard has released a critical security advisory (CVE-2025-14733, CVSS 4.x: 9.3) regarding an out-of-bounds write vulnerability. This flaw may allow a remote unauthenticated attacker to execute arbitrary code. WatchGuard has observed attackers actively attempting to exploit this vulnerability. For detailed information, please refer to the WatchGuard official website.
- Affected Platforms:
  - WatchGuard Fireware OS versions 2025.1 to 2025.1.3
  - WatchGuard Fireware OS versions 12.5 to 12.5.14
  - WatchGuard Fireware OS versions 12.0 to 12.11.5
  - WatchGuard Fireware OS versions 11.10.2 to 11.12.4+541730
- Recommended Actions:
  - Please update to the following versions:
  - WatchGuard Fireware OS version 2025.1.4
  - WatchGuard Fireware OS version 12.5.15
  - WatchGuard Fireware OS version 12.11.6
  - WatchGuard Fireware OS version 12.3.1_Update4 (B728352)
  - Note: WatchGuard Fireware OS 11.x versions have reached End of Life (EoL); it is recommended to upgrade to a supported version.
- Reference Material:
  1. https://www.twcert.org.tw/tw/cp-169-10589-329d6-1.html

Computer and Communication 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:20251223_03

Last update: **2025/12/23 13:54**