Post Date: 2026/07/16

Vulnerability AlertWatchGuard Firebox Critical Security Vulnerability (CVE-2026-13368)

- Subject: Vulnerability AlertWatchGuard Firebox Critical Security Vulnerability (CVE-2026-13368)

- Description:
  - Forwarded TWCERT/CC Security Alert TWCERTCC-200-202607-00000002
  - WatchGuard Firebox is a next-generation firewall product that provides multi-layered protection, including antivirus, IPS, APT blocking, and spam filtering. Recently, WatchGuard released a critical security vulnerability advisory (CVE-2026-13368, CVSS 4.x: 9.2). This vulnerability stems from a race condition within the LDAP authentication mechanism of Mobile User VPN with IKEv2, which subsequently leads to a Use-After-Free (UAF) vulnerability.
  - If the Firebox has Mobile User VPN with IKEv2 configured and uses an external LDAP authentication server, an unauthenticated remote attacker could exploit this vulnerability to execute arbitrary code within the context of the iked process.
- Affected Platforms:
  - Fireware OS version 2025.1
  - Fireware OS version 12.x
  - Fireware OS version 12.5.x (T15 & T13)
  - Fireware OS version 11.x
- Recommended Actions:
  - Please update to the following versions: Fireware OS version 2026.2.1, Fireware OS version 12.12.1
- References:
  1. https://www.twcert.org.tw/tw/cp-169-11022-eee7d-1.html

Computer and Communication Center
Network Systems Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260716_21

Last update: **2026/07/16 15:20**