Posted Date: 2025/11/26

[Vulnerability Alert] ASUS DSL Routers Have a High-Risk Security Vulnerability (CVE-2025-59367), Please Confirm and Patch as Soon as Possible

- Subject: [Vulnerability Alert] ASUS DSL Routers Have a High-Risk Security Vulnerability (CVE-2025-59367), Please Confirm and Patch as Soon as Possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center Security Alert NISAC-200-202511-00000204
  - Researchers have discovered an Authentication Bypass vulnerability (CVE-2025-59367) in some ASUS DSL router models.
  - An unauthenticated remote attacker can exploit this vulnerability to perform unauthorized access on the affected devices. Please confirm and patch as soon as possible.
- Affected Platforms:
  - DSL-AC51
  - DSL-AC750
  - DSL-N16
- Recommended Measures:
  - The official source has released a fix update for the vulnerability; please update to the following versions:
  - ASUS DSL-AC51 Firmware version 1.1.2.3_1010
  - ASUS DSL-AC750 Firmware version 1.1.2.3_1010
  - ASUS DSL-N16 Firmware version 1.1.2.3_1010
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10517-e8379-1.html

Computer and Communications Center
Network Systems Group