Posted Date: 2025/09/12

[Vulnerability Alert] Sophos AP6 Series Wireless Access Points have a major security vulnerability (CVE-2025-10159)

- Subject: [Vulnerability Alert] Sophos AP6 Series Wireless Access Points have a major security vulnerability (CVE-2025-10159)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000005
  - Sophos has released a major security advisory (CVE-2025-10159, CVSS: 9.8) for its AP6 series wireless access points. This is an authentication bypass vulnerability that allows an attacker to access the wireless access point's management IP address and obtain administrator privileges.
  - Note: Users with the default automatic update policy do not need to take any additional action; if automatic updates are disabled, please manually upgrade to fix this security vulnerability.
- Affected Platforms:
  - AP6 series wireless access point firmware versions before 1.7.2563 (exclusive)
- Recommended Measures:
  - Update the AP6 series wireless access point firmware to version 1.7.2563 (inclusive) or later.
- References:
  1. Resolved Authentication Bypass Vulnerability in Sophos AP6 Series Wireless Access Points Firmware (CVE-2025-10159) https://www.sophos.com/en-us/security-advisories/sophos-sa-20250909-ap6
  2. CVE-2025-10159 https://www.cve.org/CVERecord?id=CVE-2025-10159

Computer and Communications Center
Network Systems Group