POSTING DATE: 2026/01/23

[VULNERABILITY ALERT] Pro-Com | PrismX MX100 AP controller - Use of Hard-coded Credentials Vulnerability

- Subject: [VULNERABILITY ALERT] Pro-Com | PrismX MX100 AP controller - Use of Hard-coded Credentials Vulnerability

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center (TWCERTCC) Security Alert TWCERTCC-200-202601-00000020
  - [Pro-Com | PrismX MX100 AP controller - Use of Hard-coded Credentials] (CVE-2026-1221, CVSS: 9.8) The PrismX MX100 AP controller contains a Use of Hard-coded Credentials vulnerability. An unauthenticated remote attacker can use the database account and password hard-coded in the firmware to log into the database.
- Affected Platforms:
  - PrismX MX100 AP controller versions prior to v1.03.23.01 (exclusive)
- Recommended Actions:
  - Please update the firmware to version v1.03.23.01 (inclusive) or later.
- Reference Material:
  1. https://www.twcert.org.tw/tw/cp-132-10642-3b808-1.html

Computer and Communication Center
Network Systems Division, Respectfully