Post Date: 2026/06/17

□Vulnerability Alert□Cellopoint | CelloOS - Improper Access Control

- Subject: □Vulnerability Alert□Cellopoint | CelloOS - Improper Access Control

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Alert TWCERTCC-200-202606-00000013
  - □Cellopoint | CelloOS - Improper Access Control□(CVE-2026-12059, CVSS: 8.8) An Improper Access Control vulnerability exists in the SSH service of CelloOS developed by Cellopoint. An authenticated remote attacker could bypass the original command restriction mechanism, thereby executing unauthorized operating system commands.
- Affected Platforms:
  - CelloOS versions prior to 4.8.0 Build 20260316 (excluding)
- Recommended Actions:
  - The vendor released an online patch on 2026/03/18. For systems that cannot receive online updates due to being offline, isolated, or other reasons, they should be manually updated to the patched version released on or after 2026/03/18.

Computer and Communication Center
Network Systems Division