Submit #514957: China Mobile Internet of Things Enterprise Gateway GT3200-8G8P;GT3200-4G4P;ZXWT-MIG-P8G8V;ZXWT-MIG-P4G4V;P22g-CIac Execution of unauthorized command

Title China Mobile Internet of Things Enterprise Gateway GT3200-8G8P;GT3200-4G4P;ZXWT-MIG-P8G8V;ZXWT-MIG-P4G4V;P22g-CIac Execution of unauthorized command

Description Among the affected enterprise gateway devices, attackers can enable the **Telnet service on the LAN side** without authorization. Moreover, if attackers log in to the devices using the default weak passwords, they can also utilize an **effective Token** to enable the **Telnet service on the WAN side**. Due to the existence of **hard-coded credentials** for the Telnet service's authentication, attackers can escalate their privileges to root by using the **su command** after connecting to Telnet (the default password for the Telnet account is the default one), and the root password is also hard-coded. This vulnerability enables attackers to fully control the affected gateway devices, thereby endangering the overall network security.

Source ⚠️ https://github.com/Fizz-L/Vulnerability-report/blob/main/Unauthorized%20access%20to%20execute%20the%20telnet%20command.md

User FizzL (UID 82411)

Submission 03/05/2025 01:50 PM (17 days ago)

Moderation 03/17/2025 08:01 AM (12 days later)

Status Accepted

VulDB Entry 299896 [China Mobile P22g-CIac up to 20250305 Telnet Service improper authorization]

Points 20

⚠ Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

❓ Documentation

- Submission Policy
- Data Processing
- CVE Handling