COMMUNITY CONTENT

Home › Submit › 782934

Submit #782934: CampCodes Administrator Complete POS Management And Inventory System v4.0.6 remote

Title CampCodes Administrator Complete POS Management And Inventory System v4.0.6 remote

Description 1. Arbitrary Environment Variable Injection via Insufficient Sanitization:

- The backend API responsible for updating system configurations (such as Twilio SMS settings) fails to properly sanitize user input before writing it to the root `.env` configuration file.
- An authenticated attacker can insert newline characters (`\n`) within the JSON payload. When the backend processes this, it breaks out of the intended variable definition and injects arbitrary, attacker-controlled environment variables directly into the `.env` file.

2. Configuration Override via `.env` Parsing Behavior:

- The Laravel framework parses the `.env` file sequentially from top to bottom. If a variable is defined multiple times, the last occurrence takes precedence.
- By injecting into settings that are typically stored at the bottom of the `.env` file (e.g., `TWILIO_FROM`), the attacker's injected variable effectively overrides critical system variables defined earlier, such as `DUMP_PATH` (which dictates the executable path for the `mysqldump` utility).

3. Remote Code Execution (RCE) Impact:

- When an administrator triggers the "Generate Backup" function, the application reads the poisoned `DUMP_PATH` variable and concatenates it directly into a system command executed via PHP's `exec()` function without adequate escaping.
- This allows the attacker to execute arbitrary Operating System commands (e.g., `certutil`, `curl`, `whoami`) with the privileges of the Web Server (e.g., Apache/Nginx), leading to complete system compromise, data exfiltration, and unauthorized access.

Source https://github.com/whatyourname12345/CVE/tree/main/POS

User chenkh (UID 98596)

Submission 03/19/2026 11:14 AM (17 days ago)

Moderation 04/04/2026 04:04 PM (16 days later)

Status Accepted

VulDB entry [Campcodes Complete POS Management and Inventory System up to 4.0.6 Environment Variable SettingsController.php injection]

Community Content

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

Points 20