SQL Injection in Terminal Voice Audit feature of SmartVista SVFE2 version 2.2.22 (CVE-2022-38617)

CVE-2022-38617

Exploit Title: SQL Injection in Terminal Tariff Group feature of SmartVista SVFE2 version 2.2.22

Date: 26/07/2022

Exploit Author: Trong Pham aka Dtro of VietSunshine Cyber Security Services

Vendor Homepage: https://www.bpcbt.com/

Affected Version(s): SmartVista SVFE2 version 2.2.22

Description: SmartVista SVFE2 version 2.2.22 and earlier are affected by an SQL Injection vulnerability. An authenticated users could inject SQL query to "voiceAudit:j_id97" parameter in /SVFE2/pages/audit/voiceaudit.jsf to dump all databases.

Steps to reproduce:

- An attacker requires an account on the SmartVista SVFE2. An attacker can use a quote character to break query string and inject sql payload to "voiceAudit:j_id97" parameter in /SVFE2/pages/audit/voiceaudit.jsf. Response data could help an attacker identify whether an injected SQL query is correct or not.
- Example of injecting SQL to "voiceAudit:j_id97" parameter:
  - 1')or 1=1) -- ⟶ Correct query → return all data in table
  - 1')or 1=2) -- → Wrong query → return without data

Previous
SQL Injection in Terminal Tariff Group feature of SmartVista SVFE2 version 2.2.22...

Next
SQL Injection in Terminal MCC Group feature of SmartVista SVFE2 version 2.2.22 ...

Last modified 2mo ago