SQL Injection in Service Group feature of SmartVista SVFE2 version 2.2.22 (CVE-2022-38615)

CVE-2022-38615

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

Date: 26/07/2022

Exploit Author: Tin Pham aka TF1T 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 "UserForm:j_id88", "UserForm:j_id90", "UserForm:j_id92" parameters (Group ID, Service ID and Description) in /SVFE2/pages/feegroups/service_group.jsf to dump all databases.

Steps to reproduce:

- An attacker requires an account on the SmartVista SVFE2. Attacker can use a quote character to break query string and inject sql payload to "UserForm:j_id92" parameter (Description), don't use a quote character and inject sql payload to "UserForm:j_id88", "UserForm:j_id90" parameters (Group ID, Service ID), in /SVFE2/pages/feegroups/service_group.jsf. Response data could help an attacker identify whether an injected SQL query is correct or not.
- Example of injecting SQL to "UserForm:j_id92" parameter (Description):
  - 'or '1%' LIKE '1 → Correct query → Return all rows in current table
  - 'or '1%' LIKE '0 → Wrong query → Return 0 row
- Example of injecting SQL to "UserForm:j_id88", "UserForm:j_id90" parameters (Group ID, Service ID)
  - 1 or 1=1 → Correct query → Return all rows in current table

- 1 or 1=0 → Wrong query → Return 0 row

Previous
SmartVista SVFE2

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

Last modified 2mo ago