Description

Due to a lack of overall input validation, an authenticated user can inject JavaScript Cross Site Scripting payloads into fields in Axon PBX to create stored or reflected XSS conditions.

Vulnerability type

Cross Site Scripting (XSS)

Vendor

NCH Software

Affected versions

Axon PBX 2.22 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

```
Extension name (stored)
Line name (stored)
Outbound dialing plan (stored)
blacklist ip (stored)
SipRule (stored)
Primary phone (stored)
Customer name (stored)
/planprop?id= (reflected)
/extensionsinstruction?id= (reflected)
/ipblacklist?errorip= (reflected)
```

Link

https://www.nch.com.au/pbx/index.html