0xfml added Quorum XSS History

1 contributor

34 lines (22 sloc) | 756 Bytes

Description

Due to a lack of proper overall input validation, an authenticated user can inject JavaScript Cross Site Scripting payloads into fields in Quorum to create stored or reflected XSS conditions. It was observed that some basic script tags were filtered however this is easily bypassed with a slightly more diverse payload.

Vulnerability type

Cross Site Scripting (XSS)

Vendor

NCH Software

Affected versions

Quorum 2.03 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

```
User Display Name (stored)
Conference Description (stored)
/uploaddoc?id= (reflected)
/conference?id= (reflected)
/conferencebrowseuploadfile?confid= (reflected)
```

Link

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