

main



poc / NCH / IVM\_5.12\_XSS.md



Oxfml added ivm xss

History

1 contributor

36 lines (19 sloc) | 557 Bytes



Description

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

Vulnerability type

Cross Site Scripting (XSS)

Vendor

NCH Software

Affected versions

IVM Attendant v5.12 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

Mailbox name (stored)

/ogmlist?folder= (reflected)

/ogmprop?id= (reflected)

/msglist?mbx= (reflected)

Link

<https://www.nch.com.au/ivm/index.html>