Description

An authenticated user can view or delete any file on the remote system via path traversals in separate functions. This condition is however dependent on the permission level and context of the running application instance. This can also be used to view credential files of other NCH applications often stored in `\ProgramData\NCH Software\` or in conjunction with the RCE condition to validate paths needed for the zip traversal.

Vulnerability type

Directory Traversal & Arbitrary File Deletion

Vendor

NCH Software

Affected versions

IVM Attendant v5.12 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

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

`HOST/logdeleteselected [check0 param]` (delete)

Link

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