

main

...

poc / NCH / Flexiserver\_6.00\_LFI.md



Oxfml added Flexiserver LFI

History

1 contributor

30 lines (16 sloc) | 612 Bytes

...

Description

An authenticated user can view any file on the remote system via path traversals in the syslog function. 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

Vendor

NCH Software

Affected versions

Flexiserver 6.00 and earlier

Attack type

Remote

Authenticated

Yes

Attack vectors

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

Link

<https://www.nchsoftware.com/flexi/index.html>