hackerhouse-opensource / **iscsicpl_bypassUAC** Public

hackerfantastic Errata 827e242 · 2 years ago **7 Commits**

iscsicpl_BypassUAC	minor bug fix for build under release/d...	2 years ago
iscsiexe	minor bug fix for build under release/d...	2 years ago
.gitattributes	initial commit public release	2 years ago
.gitignore	initial commit public release	2 years ago
README.md	Errata	2 years ago
iscsicpl_BypassUAC.sln	initial commit public release	2 years ago

README

iscsicpl autoelevate DLL Search Order hijacking UAC Bypass 0day

The iscsicpl.exe binary is vulnerable to a DLL Search Order hijacking vulnerability when running 32bit Microsoft binary on a 64bit host via SysWOW64. The 32bit binary, will perform a search within user %Path% for the DLL iscsiexe.dll. This can be exploited using a Proxy DLL to execute code via "iscsicpl.exe" as autoelevate is enabled. This exploit has been tested against the following versions of Windows desktop:

- Windows 11 Enterprise x64 (Version 10.0.22000.739).
- Windows 8.1 Professional x64 (Version 6.3.9600).

These files are available under a Attribution-NonCommercial-NoDerivatives 4.0 International license.

About

UAC bypass for x64 Windows 7 - 11

hacker.house

Readme
Activity
791 stars
17 watching
150 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

C++ 84.6% C 15.4%